Marcel Bresink

Mac OS X / Mac OS X Server: Heterogene Netzwerke

Aktualisierung zu Mac OS X 10.4 „Tiger“

Oktober 2005

Addendum zum Buch
Mac OS X / *Mac OS X Server: Heterogene Netzwerke*, mitp-Verlag, Bonn,
ISBN 3-8266-1351-X.

Version 25. Oktober 2005

Alle Rechte, auch die der Übersetzung vorbehalten. Kein Teil des Werkes darf ohne Genehmigung des Urhebers und des mitp-Verlags Bonn verbreitet werden. Autor und Verlag übernehmen keine Gewähr für die Funktion einzelner Programme oder von Teilen derselben. Insbesondere übernehmen Autor und Verlag keinerlei Haftung für eventuelle aus dem Gebrauch resultierende Folgeschäden.

Die Wiedergabe von Gebrauchsnamen, Handelsnamen, Warenbezeichnungen usw. in diesem Werk berechtigt auch ohne besondere Kennzeichnung nicht in der Annahme, dass solche Namen im Sinne der Warenzeichen- oder Markenschutzgesetzgebung als frei zu betrachten wären und daher von jedermann benutzt werden dürfen.

© Copyright 2005 by Marcel Bresink
Gesetzt mit dem LaTeX-Dokumentensatzsystem unter Mac OS X.

Inhaltsverzeichnis

1 Vorwort **1**

2 Überblick: Neue Funktionen in Mac OS X Tiger **3**

2.1 Änderungen in der Architektur des Systems 3

2.2 Neu mitgelieferte Programme und Funktionen für Endbenutzer 5

2.3 Neu mitgelieferte Programme für den Server 6

2.4 Neue Möglichkeiten für Zugriffsrechte 7

2.5 Neue und geänderte Netzwerkfunktionen 8

2.6 Verbesserte Benutzeroberfläche auf dem Server 10

2.7 Eingeschränkte Features von Mac OS X 10.4 11

2.7.1 Aktualisierung eines Panther-Servers 11

2.7.2 Einrichten der Netzinfrastruktur 12

2.7.3 Arbeiten mit verwalteten Einstellungen 13

2.7.4 Unterstützung klassischer Mac OS-Systeme 13

2.7.5 Arbeiten mit einem zentralen Netzwerkordner für Schriftarten 13

2.7.6 Anbindung an NIS-Verzeichnisdienste 14

2.7.7 Drucken im Netz 14

2.7.8 Faxempfangsserver und Faxempfang auf Clients 14

2.7.9 Automatische Proxy-Konfiguration auf Clients 15

2.7.10 Verwendung von squid 15

2.7.11 Verwendung der NetBoot-Funktionen 15

3 Installation eines Mac OS X-Netzes **17**

3.1 Installationsplanung 17

3.2 Einsatz von AppleTalk 18

3.3 Fernverwaltung eines Tiger-Servers 19
3.4 Ablauf der Server-Installation 19

4 Einrichten der Netzinfrastruktur 23
4.1 Der DNS-Dienst 23
4.1.1 Neuerungen im weltweiten DNS-Betrieb 23
4.1.2 Einrichtung eines DNS-Servers 23
4.1.3 Einrichtung eines DHCP-Servers 27

5 Das Berechtigungskonzept in Mac OS X 31
5.1 Die neue Technik: Zugriffssteuerungslisten 31
5.2 ACLs im Detail 32
5.2.1 GUIDs und ihre Anwendung 32
5.2.2 Zugriffsoperationen 34
5.2.3 Vererbung der Einträge in der Ordnerhierarchie 35
5.2.4 Auswertung der Zugriffssteuerungseinträge 36
5.3 Wichtige Hinweise zum Einsatz von ACLs 37
5.3.1 Beschränkte Einsatzmöglichkeit 37
5.3.2 Anwendung der Zugriffssteuerung auf Dienste 37
5.3.3 Ratschläge zur Verwendung 38
5.4 Arbeiten mit ACLs 40
5.4.1 ACLs in der grafischen Oberfläche 40
5.4.2 Verschachtelte Gruppen im Arbeitsgruppen-Manager 45
5.4.3 Einstellung von SACLs 46
5.4.4 ACLs auf der Kommandozeile 47

6 Benutzer, Gruppen und Computer 53
6.1 Ortsungebundene Benutzer 53
6.1.1 Neue Funktionen 53
6.1.2 Einrichten der Synchronisationsregeln für private Dateien . . . 56
6.2 Behandlung von Kennworten in Mac OS X Tiger 59
6.2.1 Zusätzliches Verfahren zur Prüfung von Kennworten 59
6.2.2 Ausschließen bestimmter Verfahren zum Prüfen von Kennworten 60
6.3 Der neue Kennwortassistent 63

6.4 Ausfall der Kerberos-Funktionen in Tiger 64
6.5 Vordefinierte Konten 65
6.6 Arbeiten mit Gruppenordnern 66
6.6.1 Einrichten eines Gruppenordners auf einem zentralen Dateiserver 66
6.6.2 Vereinfachung des Zugriffs auf Gruppenordner für die Gruppenmitglieder 70
6.7 Verwaltete Benutzerkonten in der Standardversion von Mac OS X . . 72
6.8 Verwaltete Einstellungen für Benutzerkonten 74
6.8.1 Einrichten von Einstellungen für nicht unterstützte Programme 76
6.8.2 Die Realisierung verwalteter Einstellungen 80
6.8.3 Arbeiten mit Einstellungsmanifesten 84
6.9 Einstellungen für den Netzwerkordner des Finders 86
6.9.1 Einführung 86
6.9.2 Aufbau von verwalteten Netzwerkansichten 90
6.9.3 Erstellen einer verwalteten Netzwerkansicht 90
6.9.4 Zuweisung verwalteter Netzwerkeinstellungen an Klienten . . 94

7 Die Dateiserverfunktionen 97
7.1 Maximale Pfadlängen bei Verwendung von Automounts für Privatordner 97
7.2 Einschränkungen des NFS-Servers 98
7.3 Über AFP auf NFS: Resharing 99
7.4 Der CIFS/SMB-Server 100
7.4.1 Sicherungs-Domänen-Controller 100
7.4.2 Neue Identifizierungsmethoden 102
7.5 Probleme in gemischten Netzen 103
7.5.1 Kompatibilitätsprobleme des NFS-Automounters 103
7.6 Unerwünschten Kerberos-Einsatz verhindern 104

8 Verzeichnisdienste 107
8.1 Unterstützte Informationskategorien 107
8.2 Quellen für Verwaltungsinformationen 107
8.3 Das Lookup-Subsystem 107
8.4 Das Programm Verzeichnisdienste 109

8.5 Die Anbindung an NIS 109
8.6 NetInfo – der klassische Verzeichnisdienst 109

9 LDAP und Apple Open Directory 111
9.1 LDAP in Mac OS X Server nutzen 111
9.1.1 Überwachung und Konfiguration des LDAP-Servers 111
9.1.2 Die abgesicherte Bindung zwischen Server und Klienten 114
9.1.3 Weitere Sicherheitsmerkmale 117
9.2 Arbeiten mit dem LDAP-Browser 119
9.3 Arbeiten mit Zertifikaten 119
9.3.1 Das neu gestaltete Schlüsselbund-Programm 119
9.3.2 Ungültigwerden von Zertifikaten 123
9.3.3 Erzeugen eines Spielzertifikats zum SSL-Zugriff auf den LDAP-Server 125
9.3.4 Eine private Zertifizierungsstelle einrichten 128

10 Drucken im Netz 139
10.1 Verwendung von USB-Druckern an Airport-Basisstationen 139
10.2 IPP als Übertragungsprotokoll der Wahl 139
10.3 Verbesserungen im Server Admin-Programm 139
10.4 Neue Features auf Client-Seite 140

11 E-Mail – die elektronische Post 143
11.1 Einführung 143
11.1.1 Korrektur 143
11.1.2 Überblick über die Neuerungen 143
11.1.3 Aktualisierung der Mail-Dienste 144
11.2 Einrichtung des Mail-Servers 144
11.2.1 Basiseinstellungen 144
11.2.2 Kontingentierung 145
11.2.3 Wartungsarbeiten über Server Admin 146
11.3 Filterung von E-Mail 148
11.3.1 Allgemeines 148
11.3.2 Ausfiltern von unerwünschter Werbepost 148
11.3.3 Ausfiltern von Computerviren 154

12 Web-Dienste 157
12.1 Nutzung eines Proxy-Cache-Servers 157
12.1.1 Arbeiten mit automatischer PAC-Konfiguration 157
12.1.2 Alternative Lösungen für Proxy und Inhaltsfilterung 159
12.1.3 Konfiguration von DansGuardian 160
12.2 Apples Erweiterungsmodule zu Apache 162
12.3 Der Weblog-Dienst Blojsom 163
12.3.1 Einrichten des Weblog-Dienstes 164
12.3.2 Aufruf der Weblog-Funktion 166
12.3.3 Terminologie und Funktionen des Bloggens 166
12.4 Instant Messaging mit dem iChat-Server 171
12.4.1 Einführung 171
12.4.2 Einrichten des Chat-Servers 173
12.4.3 Verwendung von iChat 174
12.5 QuickTime Streaming Server 177
12.5.1 Neuerungen 177
12.5.2 Fallbeispiele: Streaming und Erzeugung von Webseiten 179

13 Fernstart – die NetBoot-Funktion 185
13.1 Änderungen in Server Admin 185
13.2 Das neue System-Image-Dienstprogramm 185
13.3 Image-Dateien pflegen und anpassen 189
13.3.1 Hinzufügen von Paketen zu einem vorhandenen Image 190
13.3.2 Hinzufügen durch Synchronisation 192

14 Fortgeschrittene Netzfunktionen 193
14.1 Der neue Software-Aktualisierungsdienst 193
14.1.1 Einführung 193
14.1.2 Einrichten der Software-Aktualisierungsfunktion 195
14.2 Verschlüsselte Teilnetze mit VPN 198

Kapitel 1

Vorwort

Anders als ursprünglich geplant, erscheint die Aktualisierung des Buches *Mac OS X / Mac OS X Server: Heterogene Netzwerke* für Apples neues System Mac OS X 10.4 Tiger mit einiger Verspätung. Verantwortlich hierfür war leider der Zustand, in dem Apple das neue Tiger-System, insbesondere in der Serverversion, in den Markt eingeführt hatte. Zwar ließen sich die ersten Systemversionen im privaten Umfeld – also für den überwiegend häuslichen Gebrauch auf einem Familiencomputer – recht gut einsetzen und das Betriebssystem lief dank seines Unix-Unterbaus selbstverständlich sehr stabil, jedoch stellten viele Profianwender schon nach kurzer Zeit fest, dass der Einsatz in einem größeren Netzwerk, erst recht in einer heterogenen Umgebung, einige technische Schwierigkeiten mit sich bringen konnte.

Für viele Anwender, die ein Mac OS X-Netz in einem Unternehmen einsetzen, waren die Versionen 10.4 und 10.4.1 daher ein großes Problem, denn viele Systemfunktionen, die mit Panther noch einwandfrei ihren Dienst verrichteten, funktionierten in Tiger nur noch fehlerhaft oder überhaupt nicht mehr. Schon das erfolgreiche Update eines Servers von Panther auf Tiger kann eine größere Hürde sein, denn je nachdem, welche Dienste auf dem Server aktiviert sind, bleibt das System bereits beim ersten Start stehen und es kann sich ein Totalausfall ergeben, der nur mit erheblichen Systemkenntnissen beseitigt werden kann.

Die Aktualisierung auf Mac OS X 10.4.2 und das Sicherheits-Update 2005-07 Version 1.1 zeigten einen ersten Schritt in die richtige Richtung. Mehr als 100 der schlimmsten Produktmängel und mehr als 35 Sicherheitslücken wurden beseitigt. Trotzdem sind auch mit diesem Release-Stand immer noch nicht alle Probleme behoben. Spezielle Funktionen, wie zum Beispiel die Einbindung in NIS-Netzwerke sind immer noch nicht verwendbar, andere ursprünglich angekündigte Features, wie etwa die neue Grafiktechnologie *Quartz Extreme 2D*, sind immer noch nicht freigeschaltet. Einige Komponenten scheinen überhastet zusammengestellt worden zu sein. So fehlt beispielsweise auf der Server-DVD der größte Teil der deutschsprachigen Anpassung des Programms *System Profiler*, während diese auf der DVD der Standardversion mitgeliefert wird. Apple scheint schlicht vergessen zu haben, die hierfür nötigen Dateien mit auf die DVD zu packen.

Ab der Version 10.4.3 — die sich im Moment noch in der Entwicklung befindet — werden Gerüchten zufolge zwischen 500 und 1.000 Produktmängel behoben sein, so dass hier mit einer Besserung der allgemeinen Lage zu rechnen ist. Wie immer steht diese zukünftige Version jedoch unter großer Geheimhaltung und Apple droht mit juristischen Schritten, falls Informationen über Vorabversionen von 10.4.3 publik werden. Auch ein Zeitplan für die Veröffentlichung steht noch nicht fest.

Über die voraussichtlich erste auch für heterogene Netzwerke brauchbare Version von Mac OS X Tiger Server kann und darf daher noch nicht berichtet werden. Mit 10.4.2 liegt jedoch eine vorläufige Fassung vor, die zumindest in Teilen einsetzbar ist und bereits von einigen Anwendern verwendet wird, die auf den Umstieg zu Tiger gezwungen sind, weil für Neuinstallationen Panther nicht mehr im Handel erhältlich ist, oder weil sie neue Hardware gekauft haben, auf denen sich Mac OS X Panther nicht mehr installieren lässt.

Die nachfolgenden Abschnitte gehen deshalb auf Version 10.4.2 des Betriebssystems ein, so wie es bei Redaktionsschluss Mitte Oktober 2005 vorlag. Hierbei wird versucht, die gleiche Reihenfolge der Themen wie im Hauptbuch *Heterogene Netzwerke* beizubehalten.

Kapitel 2

Überblick: Neue Funktionen in Mac OS X Tiger

Mac OS X 10.4 stellt eine Reihe neuer und geänderter Funktionen zur Verfügung. Dies betrifft sowohl die innere Architektur des Systems, als auch die mitgelieferten Programme.

2.1 Änderungen in der Architektur des Systems

Das Tiger-Betriebssystem unterstützt nun die *64-Bit-Technologie* so gut wie vollständig. Die innere Aufbau der von Apple bisher verwendeten PowerPC-Prozessoren war immer schon auf 64 Bit ausgerichtet, seit der fünften Generation (G5) steht mit dem IBM PPC 970 jedoch auch ein Prozessor für Macintosh-Systeme zur Verfügung, der die Verwendung von 64 Bit in noch größerem Umfang, insbesondere auch für die Adressierung des Hauptspeichers beherrscht. Für die Praxis heißt das, dass ein laufendes Programm nun mehr als 4 GByte Speicher vom System anfordern darf. Besonders für große Datenbanksysteme in professionellen Netzwerken ist dies ein entscheidender Schritt, da es hierdurch möglich wird, z.B. Teile einer Datenbank, besonders deren Suchindex, im Hauptspeicher zu halten, so dass beim Zugriff nicht ständig auf die Festplatte zugegriffen werden muss. Dies kann zu enormen Geschwindigkeitssteigerungen führen. Für Programme, die nicht ständig mit sehr großen Datenmengen arbeiten, ergibt sich jedoch so gut wie kein Vorteil aus der 64-Bit-Technik.

Um mehr als 4 GByte Speicher ansprechen zu können, müssen die Programme entsprechend angepasst sein: Die Adressen, um die einzelnen Speicherstellen auswählen zu können, werden von 32 Bit auf 64 Bit erweitert. Bei den Systemkomponenten von Mac OS X ist dies so gelöst, dass Apple die einzelnen Codebibliotheken, die die Funktion des Betriebssystems ausmachen, in zwei verschiedenen Versionen, eine für 32, eine für 64 Bit mitliefert, so dass sich die Programme den für

sie passenden Code heraussuchen können. Aus technischen Gründen lässt sich die Adressierung innerhalb eines laufenden Programms nicht zwischen 32 und 64 Bit mischen, so dass jeder Prozess sich strikt in einer der beiden Betriebsarten befinden muss. Zur Kompatibilität mit älteren Programmen werden die 32-Bit-Module des Betriebssystems noch für viele Jahre erhalten bleiben. Alle Komponenten für die grafische Oberfläche zum Beispiel stehen mit Absicht noch nicht in einer 64-Bit-Variante zur Verfügung, da die 64-Bit-Technik hier keine Vorteile bringt, eher sogar Nachteile, da die doppelt so langen Adressen mehr wertvollen Speicherplatz verbrauchen würden. Als Konsequenz kann die 64-Bit-Adressierung in Mac OS X 10.4 nur für nicht-grafische Programme genutzt werden. Ein Programm mit grafischer Oberfläche, das trotzdem 64-Bit-Technik nutzen soll, muss daher in ein Front-End in 32-Bit-Technik und ein Back-End mit 64 Bit geteilt werden und beide Hälften müssen über eine Schnittstelle miteinander kommunizieren.

Die Trennung der Programmkomponenten in 32 und 64 Bit macht es auch möglich, den Code so zu optimieren, dass andere Vorteile der G5-Architektur, wie z.B. dessen geänderte AltiVec-Architektur genutzt werden können. Apple verwendet für einige Tiger-Programme hierzu die Fat Binary-Technik, also die Möglichkeit, unterschiedliche Codes für verschiedene Prozessortypen in ein und derselben Programmdatei unterzubringen. So gibt es in Tiger Programmdateien, die zum einen 32-Bit-Code für G3- und G4-Computer, zum anderen zusätzlich noch 64-Bit-Code für G5-Computer enthalten.

Einen weiterer großer Eingriff in die Architektur des Systems wird unter anderem beim Start eines Tiger-Computers wirksam: Es gibt einen neuen übergeordneten Startdienst mit dem Namen *launchd (Launch Daemon)*, der sowohl für das Betriebssystem als auch für einzelne Benutzer den Start von Hintergrundprogrammen und -diensten überwacht und organisiert. Launchd ist eine Eigenentwicklung von Apple und soll die bisherigen Unix-Dienste *mach_init* (Start des Systemkerns), *init* (Start des Betriebssystems), *xinetd* (Start von Netzdiensten) und *cron* (termingesteuerter Programmstart) auf lange Sicht ablösen. Vorteil von launchd ist, dass die zahlreichen Konfigurations- und Skriptdateien, die für all diese unterschiedlichen Startmechanismen zuständig sind, vereinheitlicht und an einem zentralen Punkt zusammengefasst werden können. Der launchd-Dienst verwendet die in Mac OS X üblichen *plist-Dateien (Property Lists)* im XML-Format, um die Konfiguration zu speichern.

Das Programm launchd übernimmt auch weitere Aufgaben. So kontrolliert es unter anderem, ob die Dienstprozesse in Mac OS X korrekt arbeiten und sich „normal" verhalten. Stürzt ein Prozess unerwartet ab, so wird der Dienst automatisch wieder neu gestartet (Abbildung 2.1).

Nachteil der neuen launchd-Technik ist, dass die XML-Konfigurationsdateien in beschränkten Umgebungen, z.B. bei der Verwendung eines Kommandozeileneditors über eine SSH-Verbindung hinweg, nur sehr schwer gewartet werden können, da sie mehr syntaktische Markierungen als eigentliche Informationen speichern. Salopp gesagt: Vor lauter XML-Tags ist der Inhalt kaum noch sichtbar. Zudem scheint die neue Technik voller Kinderkrankheiten zu stecken, was unter anderem für einige Probleme der ersten Tiger-Versionen mitverantwortlich ist. Apple verwendet

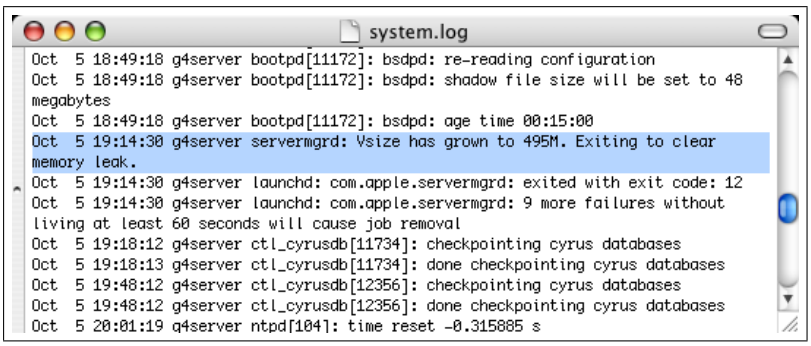
system.log
Oct 5 18:49:18 g4server bootpd[11172]: bsdpd: re-reading configuration
Oct 5 18:49:18 g4server bootpd[11172]: bsdpd: shadow file size will be set to 48 megabytes
Oct 5 18:49:18 g4server bootpd[11172]: bsdpd: age time 00:15:00
Oct 5 19:14:30 g4server servermgrd: Vsize has grown to 495M. Exiting to clear memory leak.
Oct 5 19:14:30 g4server launchd: com.apple.servermgrd: exited with exit code: 12
Oct 5 19:14:30 g4server launchd: com.apple.servermgrd: 9 more failures without living at least 60 seconds will cause job removal
Oct 5 19:18:12 g4server ctl_cyrusdb[11734]: checkpointing cyrus databases
Oct 5 19:18:13 g4server ctl_cyrusdb[11734]: done checkpointing cyrus databases
Oct 5 19:48:12 g4server ctl_cyrusdb[12356]: checkpointing cyrus databases
Oct 5 19:48:12 g4server ctl_cyrusdb[12356]: done checkpointing cyrus databases
Oct 5 20:01:19 g4server ntpd[104]: time reset -0.315885 s

Abbildung 2.1: Ein Blick ins Systemprotokoll zeigt, dass launchd auch gute Eigenschaften hat: Fehlerhaft arbeitende Prozesse, die sich abnormal verhalten, werden neu gestartet. Das Programm servermgrd, das im Hintergrund die Dienste für das Programm Server Admin erbringt, ist in den ersten Tiger-Version so verheerend programmiert, dass es nach ein paar Stunden Laufzeit den kompletten Speicher des Servers aufbraucht. Das Programm merkt das und beendet sich. In diesem Fall erkennt launchd das Problem und startet den fehlerhaften Prozess automatisch neu.

launchd, um einen aggressiv optimierten Systemstart zu ermöglichen, bei dem die einzelnen Systembestandteile parallel, nur mit wenig gegenseitiger Synchronisation hochgefahren werden. Dies ermöglicht auf einem Einzelplatzcomputer zwar sehr schnelle Startzeiten von unter 30 Sekunden, was Mac OS X Tiger auf den ersten Blick sehr gut aussehen lässt, im Netzwerk sieht dies jedoch ganz anders aus. Durch mangelnde Abstimmung untereinander scheinen die Prozesse in zufälliger Reihenfolge gestartet zu werden, wodurch sie oft in der falschen Abfolge aufeinander warten und sich so große Verzögerungen beim Start ergeben. Teilweise sind Wartezeiten über 2 Minuten feststellbar, bis das Anmeldefenster erscheint, in den ersten Tiger-Versionen war in Netzwerken oft überhaupt kein zuverlässiger Systemstart möglich.

2.2 Neu mitgelieferte Programme und Funktionen für Endbenutzer

Apple liefert Mac OS X 10.4 mit neuen Features auf der Benutzeroberfläche aus, die sich an Endanwender richten. Für den Serverbetrieb sind vieler dieser Funktionen jedoch uninteressant.

Spotlight: Die frühere Indexfunktion des Finders wurde durch ein neu entwickeltes Bündel von Index- und Suchdiensten mit dem Namen *Spotlight* ersetzt, die nun etwas näher an das Dateisystem gebunden sind und systemweit allen Anwendungen zur Verfügung stehen. Der Finder und die Menüleiste

des Systems unterstützen Spotlight durch neue Benutzerschnittstellen. In der Server-Version von Mac OS X ist Spotlight standardmäßig abgeschaltet, da die Verwendung hier zu starken Geschwindigkeitseinbußen oder Fehlfunktionen führen würde.

Dashboard: Mit *Dashboard* führt Apple einen auf Web-Technologien basierenden Dienst ein, der es ermöglicht, dass Kleinstprogramme, in der Regel zur aktuellen Informationspräsentation, per Knopfdruck auf einer zweiten Bildschirmebene ein- und ausgeblendet werden können. Diese zweite Ebene zieht sich wie eine Folie über die normale grafische Arbeitsfläche und ermöglicht es, Helferprogramme, die im Hintergrund bereit gehalten werden, sehr schnell zu aktivieren und wieder vom Schirm verschwinden zu lassen.

RSS-Integration: Die Internet-Technik mit der Bezeichnung *RSS (Really Simple Syndication)* ist nun in die Web-Bibliotheken des Betriebssystems integriert und lässt die Nutzung in verschiedenen Programmen und Systemkomponenten, wie z.B. dem Webbrowser Safari zu. RSS ermöglicht es, Web-Inhalte auf einfache Weise zu veröffentlichen und zu verbreiten und diese Inhalte in Form von Nachrichten-Feeds sammeln, lesen und zusammenfassen zu können.

Automator: Das Programm *Automator* ermöglicht es Endanwendern, auch ohne Programmier- oder Skriptkenntnisse verschiedene Anwendungen automatisiert zu steuern und damit vorher festgelegte Arbeitsabläufe definieren zu können.

Kindersicherung: Die Möglichkeit, Benutzer auch auf einem Einzelplatzsystem zu verwalten und deren Umgebung auch über die Definitionen von Unix-Berechtigungen hinaus einschränken zu können, wurde erweitert und ist in ein neues Kindersicherungskonzept integriert worden.

Intelligente Ordner im Finder: Der Finder ermöglicht es, virtuelle Ordner anzulegen, die sich nicht auf einen konkreten Ordner im Dateisystem beziehen, sondern stattdessen definierte Suchabfragen darstellen, mit denen in Echtzeit eine Sicht auf ausgewählte Dateiobjekte zusammengestellt wird. So kann beispielsweise ein virtueller Ordner erstellt werden, in dem sich alle JPEG-Bilder, die jeweils in der vergangenen Woche geändert wurden, befinden.

Grapher: Das Programm *Grapher* ist eine mathematische Anwendung, mit der sich zwei- und dreidimensionale Funktionen grafisch darstellen lassen.

VoiceOver: Mit der *VoiceOver*-Technik können visuell eingeschränkte Anwender sich Textinhalte und Systemdialoge akustisch vorlesen lassen. Diese Funktion ist im Moment nur für den englischsprachigen Markt interessant, da andere Sprachen nicht berücksichtigt werden.

2.3 Neu mitgelieferte Programme für den Server

Auch serverseitig hat Apple die Anzahl der mitgelieferten Dienste und Programme erweitert. Dies betrifft unter anderem die folgenden Punkte:

Xgrid: Die früher nur im Internet von Apples Forschungsabteilung herunterladbare Umgebung *Xgrid* zum Selbstprogrammieren und Verwalten im Netz verteilter Anwendungen ist nun offizieller Bestandteil von Mac OS X Server geworden. Xgrid ermöglicht es, einen Pool von Computern zu einem Rechencluster zusammenzufassen, wobei die einzelnen Systeme gemeinsam an einem Problem arbeiten. Xgrid erfordert speziell entwickelte Software und richtet sich überwiegend an technisch-wissenschaftliche Anwender, die selbst programmieren.

WebObjects-Laufzeitumgebung: Apples Applikationsumgebung für selbst entwickelte web-basierte Anwendungen *WebObjects* wird nun als offizieller Bestandteil von Mac OS X Server mit einer unbeschränkten Nutzungslizenz ausgeliefert. Es ergänzt die JBoss- und Tomcat-Umgebungen.

Spam-Filter: Die Maildienste wurden um das freie Programm *SpamAssassin* erweitert, das unerwünschte Werbepost bereits auf dem Server zentral ausfiltern kann.

Viren-Filter: Ebenso als Ergänzung der Maildienste stellt Apple das freie Programm *ClamAV* als Antivirenlösung bei der Weiterleitung elektronischer Post für den Tiger-Server bereit.

Weblog-Dienste: Um die neumodische Technik des Bloggens, also des Veröffentlichens von aktuellen Informationen auf einem elektronischen Schwarzen Brett mithilfe der RSS- und Atom XML-Technik verwenden zu können, liefert Apple das freie Programm *Blojsom* mit.

Instant-Messaging-Dienste: Zum Austausch elektronischer Nachrichten in Echtzeit zwischen identifizierten Benutzern von Macintosh-, Windows- oder Linux-Systemen stellt Apple einen Chat-Server als Bestandteil von 10.4 zur Verfügung. Der auch als *iChat-Server* bezeichnete Dienst wird vom freien Programm *jabberd* realisiert.

Software-Aktualisierungsdienst: Es kann eine Art Proxy-Server eingerichtet werden, der im Hintergrund alle verfügbaren Software-Update-Pakete von Apple sammelt und diese zentral einem ganzen lokalen Netzwerk zur Verfügung stellt. Die Update-Funktion kann dabei für die Klienten transparent konfiguriert werden, d.h. auf einem Client-Computer kann wie vorher die Funktion Software-Aktualisierung des Programms Systemeinstellungen verwendet werden.

2.4 Neue Möglichkeiten für Zugriffsrechte

Neben den klassischen Unix-Zugriffsrechten unterstützt Mac OS X zusätzlich nun auch *Zugriffssteuerungslisten (Access Control Lists, ACLs)*, die eine noch feiner gegliederte Steuerung des Zugriffs auf Dateisystemobjekte und Dienste möglich

machen. Die ACL-Technik ist darüber hinaus kompatibel mit den von Windows-Systemen verwendeten Berechtigungen. Im einzelnen ergeben sich hierdurch folgende neue Möglichkeiten:

- Die Prüfung der Gruppenmitgliedschaft ist nicht mehr nur auf den Kurznamen einer Gruppe beschränkt, sondern auch der Langname kann herangezogen werden.
- Neben Rechten des Zugriffs können nun auch Verbote des Zugriffs ausgesprochen werden.
- Nicht nur die Parteien Eigentümer, Eigentümergruppe und Jeder können für die Definition einer Zugriffserlaubnis verwendet werden, sondern beliebige Listen von Benutzer- oder Gruppenkonten.
- Gruppenmitgliedschaften dürfen verschachtelt werden.
- Zugriffsrechte können nun von Ordnern über eines von vier einstellbaren Verfahren auf im Ordner enthaltene Objekte vererbt werden.
- Neben Schreib-, Lese-, Ausführungs- und Auflistungsrechten gibt es feiner gegliederte Rechte für den Zugriff auf die Berechtigungsattribute selbst, den Zugriff auf die Eigentümervermerke und verschiedene Löschungsprivilegien.
- Nicht nur Dateisystemobjekte, sondern auch bestimmte Netzwerkdienste können mit ACL-Berechtigungen versehen werden.

2.5 Neue und geänderte Netzwerkfunktionen

Neben den komplett neuen Programmen wurden viele bestehende Funktionen überarbeitet und durch neue Features ergänzt.

Link Aggregation: Ist ein Servercomputer mit mehreren Netzwerkanschlüssen ausgestattet, so lassen sich nun mehrere physische Anschlüsse unter dem Stichwort *Link Aggregation* zu einem einzelnen virtuellen Anschluss (mit einer einzigen Adresse) zusammenfassen, um die Leistung zu steigern.

VPN zwischen Netzwerken: Während in Panther nur die Möglichkeit bestand, sich mit einem einzelnen Rechner per VPN in ein Netzwerk einzuwählen, bietet Tiger die Möglichkeit, zwei lokale Netze über eine verschlüsselte Kommunikationsverbindung miteinander zu koppeln *(Site to Site Virtual Private Networking)*.

LDAPv3-Vertrauensstellung: Bei der Bindung von Open Directory-Klienten über das LDAPv3-Protokoll an einen Verzeichnisdienst-Server kann nun eine abgesicherte Vertrauensbeziehung definiert werden. Sicherheitslücken, die durch gefälschte Clients entstehen können, werden vermieden, indem sich beide Kommunikationspartner bei der ersten Kontaktaufnahme als echt identifizieren müssen.

Erweiterte Kerberos-Funktionen: Mehr Dienste als in Panther wurden kerberisiert, so dass sie nun Bestandteil der Gesamt-Authentifizierung (Single Sign-On) sind.

LDAP-Schemareplikation: Nicht nur die LDAP-Datenbank selbst, sondern auch die Metabeschreibung ihrer Organisation, das LDAP-Schema, kann zwischen verschiedenen LDAP-Servern repliziert werden.

Synchronisation privater Ordner für ortsungebundene Benutzer: Mit gewissen Einschränkungen unterstützt Tiger Server nun den automatischen Abgleich des privaten Ordners mobiler Benutzer. Ausgewählte Inhalte können zwischen der Platte eines portablen Computers und einem zentralen Ordner eines Dateiservers in beide Richtungen synchronisiert werden.

Verwaltete Ansicht des Netzwerkordners: Die Präsentation der Daten über das Symbol Netzwerk des Finders lässt sich nun zentral über einen Verzeichnisdienst konfigurieren.

Definition von Einstellungsmanifesten für Drittanbieterprogramme: Wenn Sie die Funktionen der verwalteten Benutzerkonten verwenden, können nicht nur Vorgaben für Einstellungen von Mac OS X gemacht werden, es lassen sich nun beliebige Einstellungen auch anderer Programme zentral vorgeben.

Vereinheitlichte Dateisperren: Wenn Sie auf einem Dateiserver sowohl das AFP- als auch das CIFS/SMB-Protokoll zum Sharing im heterogenen Netzwerk nutzen, werden Dateisperren (Locks) jetzt auch über Protokollgrenzen hinweg vom Server beachtet. Wenn z.B. ein Macintosh-Benutzer und ein Windows-Benutzer gleichzeitig auf die gleiche Datei des Servers zugreifen, wird einer der Zugriffe jetzt sauber gesperrt, so dass die Datei nicht durch gleichzeitigen Zugriff beschädigt werden kann.

Betrieb als Backup-Domänencontroller: Beim Betrieb in einem Netz mit Windows-NT-Domänen kann Mac OS X nicht nur als primärer Domänencontroller (PDC), sondern nun auch als Replikat eines solchen Servers, als Backup-Domänencontroller (BDC) konfiguriert werden.

Mitgliedsserver einer Active-Directory-Domäne: Ein Mac OS X Server kann nun Mitgliedsserver einer bestehenden Active-Directory-Domäne (Windows 2000 oder 2003 Server) werden.

Unterstützung von NTLM Version 2: Neben den Identifizierungsmethoden LAN Manager und NTLM, die in Windows-Netzwerken zur Kennwortüberprüfung eingesetzt werden, unterstützt Tiger jetzt auch die Nachfolgetechnik NTLMv2.

Virtuelle Hosts bei der E-Mail-Weiterleitung: Der Tiger-Server ist nun innerhalb gewisser Grenzen in der Lage, mehrere DNS-Domänen auf einem einzelnen Computer zu verwalten, ohne dass Anpassungen über die Kommandozeile erfolgen müssen. Ein und derselbe Computer kann als E-Mail-Server für mehrere Domains fungieren.

Vollständige Integration von CUPS: Alle Druckdienste sind nun vollständig auf CUPS umgestellt, so dass keine Altlasten mehr vorhanden sind. Der Netzwerkdruck über das moderne Protokoll IPP ist nun der empfohlene Standard. Der Server kann zusätzlich Deckblätter für Druckaufträge erstellen.

Neue Technologien für QuickTime Streaming: Der QuickTime Streaming Server unterstützt einige neue Technologien zur Datenkompression wie H.264, das Senden von HD-Filmen oder Datenströme im 3GPP-Format.

2.6 Verbesserte Benutzeroberfläche auf dem Server

Viele Bestandteile des Servers, die bisher nur über die Kommandozeile verwaltet werden konnten, lassen sich jetzt auch über die grafische Oberfläche bedienen. Dies betrifft im einzelnen die folgenden Punkte:

Gateway-Assistent: Soll ein Servercomputer als TCP/IP-Gateway konfiguriert werden (umgangssprachlich auch als „Router" bezeichnet), so kann die Einrichtung der entsprechenden Netzumgebung mit den Diensten DHCP, DNS, NAT, VPN und dem Paketfilter jetzt über ein grafisches Assistentenprogramm erfolgen.

Erweiterte DNS-Konfiguration: Die Konfiguration des DNS-Server BIND über die grafische Oberfläche hat nun weitergehende Funktionen und ist nicht mehr so fehlerhaft wie in Panther. Allerdings stehen immer noch nicht alle Funktionen in grafischer Form zur Verfügung.

Statische DHCP-Adressverteilung: Um statische IP-Adressen für den DHCP-Dienst zu konfigurieren, steht jetzt eine Eingabemöglichkeit in den Administrationsprogrammen bereit. Es ist nicht mehr nötig, direkt Einträge der NetInfo-Datenbank zu ändern.

Archivieren und Replizieren der LDAP-Datenbank: Im Zusammenhang mit den Open Directory-Verzeichnisdienstfunktionen können nun verschiedene Wartungsarbeiten an der LDAP-Datenbank direkt über das Programm Server Admin ausgeführt werden.

Kontaktinformationen für Benutzerkonten: In der LDAP-Datenbank können nun neben den eigentlichen Benutzerdaten auch Kontaktinformationen der einzelnen Benutzer, wie zum Beispiel Telefonnummern, direkt über den Arbeitsgruppen-Manager eingegeben werden.

NFS to AFP-Resharing: Die Verwendung eines Mac OS X Servers als Gateway, um über das AFP-Protokoll auf NFS-Server zuzugreifen, kann nun direkt im Arbeitsgruppen-Manager eingerichtet werden und erfordert nicht mehr die Verwendung der Kommandozeile.

Verbesserte Mailserver-Schnittstelle: Verschiedene Wartungs- und Verwaltungsfunktionen im Zusammenhang mit Postverteilungsservern, die bisher nur über

die Kommandozeile verfügbar waren, können nun über das Server Admin-Programm aufgerufen werden.

CUPS-Protokolle: Die Protokolle der Druckserver-Funktionen können nun auch auf niedrigeren Systemebenen über die Programme zur Serververwaltung eingesehen werden.

Zertifikatsverwaltung: Digitale Zertifikate lassen sich nun über eine Funktion des Server Admin-Programms verwalten. Ebenso können Unterzeichnungsforderungen (Certficate Signing Requests) bequem zum Weitergeben an eine Zertifizierungsstelle vorbereitet werden.

QuickTime Streaming Server (QTSS): Die Benutzeroberfläche des QTSS wurde vollständig überarbeitet. Zusätzlich ist der Einsatz von AppleScript möglich.

Einrichtung des Paketfilters: Die grafische Oberfläche zur Einrichtung des Paketfilters („Firewall") wurde erweitert und verbessert.

NT-Migration: Das Ersetzen eines Windows NT-Servers durch einen Mac OS X Server wird nun direkt auf der grafischen Oberfläche unterstützt. Apple stellt ein eigenes Handbuch für diese Funktion bereit.

2.7 Eingeschränkte Features von Mac OS X 10.4

Bei den nachfolgend genannten Funktionen ist Vorsicht geboten, falls Sie jetzt bereits ein heterogenes Netzwerk auf die Tiger-Version umstellen möchten. Sollten Sie auf eine dieser Funktionen angewiesen sein, so ist dringend zu empfehlen, im Moment noch auf Tiger zu verzichten, sofern möglich. Bei einigen Punkten werden mögliche Lösungen genannt. Die einzelnen Punkte werden in der Reihenfolge aufgeführt, in der das Buch *Heterogene Netzwerke* gegliedert ist. Die Problemliste erhebt keinen Anspruch auf Vollständigkeit.

2.7.1 Aktualisierung eines Panther-Servers

Die automatische Aktualisierung eines Servers, der unter Mac OS X Server 10.3.9 läuft, ist in bestimmten Installationen nur eingeschränkt oder nur mit vielen Nacharbeiten möglich, da die Konfigurationen einiger Systemdienste nicht richtig auf den neuesten Stand gebracht werden. Beachten Sie die folgenden Punkte:

Führen Sie auf jeden Fall eine vollständige Datensicherung vor der Aktualisierung durch und richten Sie sich auf eine längere Außerbetriebnahme des Netzes ein.

Prüfen Sie, ob es Ihnen nicht möglich ist, statt einer Aktualisierung den vorübergehenden Parallel- und Probebetrieb eines zweiten Servers einzurichten. Auf dem zweiten Server kann eine Neuinstallation von Mac OS X 10.4. Server vorgenommen werden und nach erfolgreicher Einrichtung können die Arbeitsdaten vom alten Server auf den neuen von Hand migriert werden.

Ist dies nicht möglich, prüfen Sie, ob statt einer Aktualisierung nicht die Installationsart ARCHIVIEREN UND INSTALLIEREN eingesetzt werden kann. Sie müssen in dem Fall Teile der Konfiguration von Hand nachführen und Benutzerdaten möglicherweise manuell wieder aus der Archivkopie in das laufende System zurück kopieren.

Falls Sie eine Aktualisierung (also keine Neuinstallation) durchführen, laden Sie vorher das Handbuch *Mac OS X Server Aktualisieren und Migrieren auf Version 10.4* unter der Adresse

`http://images.apple.com/movies/euro/de/server/documentation/pdfs/2005/Migration_v10.4.pdf`

herunter. Selbst wenn die automatische Aktualisierung funktioniert, müssen Sie die folgenden Punkte von Hand nacharbeiten:

- Aktualisieren Sie alle Gruppenkonten, indem Sie die Gruppen im Arbeitsgruppen-Manager auswählen und den Punkt ÜBERKOMMENE GRUPPE AKTUALISIEREN auswählen.
- Falls Sie SSL-Zertifikate eingesetzt haben, prüfen Sie die Zertifikate in Server Admin und importieren Sie sie eventuell neu.
- Kontrollieren Sie die Konfigurationen aller Web-Dienste und aller Druckdienste. Ist die Anzahl der Drucker gering, lohnt es sich eventuell, die Konfiguration der Druckdienste komplett zu löschen und neu anzulegen, sollte sie fehlerhaft arbeiten.

2.7.2 Einrichten der Netzinfrastruktur

Der DNS-Dienst von Mac OS X 10.4 Server startet in vielen Fällen sehr unzuverlässig. Sie sollten nach jedem Systemstart von Hand kontrollieren, ob der DNS-Server läuft, beispielsweise durch Eingabe von

```
host <name-des-servers>
```

in der Kommandozeile. Kann das System seinen eigenen Servernamen nicht mehr auflösen, so ist der Start des DNS-Dienstes fehlgeschlagen. Dies kann in einer Kettenreaktion dazu führen, dass fast alle anderen Netzdienste auf dem Server und auf allen Clients ausfallen. Versuchen Sie in diesem Fall zunächst eine Neuinitialiserung des DNS-Dienstes durch Eingabe von

```
sudo killall -HUP named
```

was das Problem bis zum nächsten Systemstart behebt. Sind allerdings mehrere andere Netzdienste durch den Ausfall von DNS in Mitleidenschaft gezogen worden und „hängen“ nun, starten Sie lieber den kompletten Server neu. Wiederholen Sie in diesem Fall den Start des Systems so oft, bis der DNS-Server auf Anhieb funktioniert. Es ist unklar, wann Apple diesen schweren Fehler behebt.

2.7.3 Arbeiten mit verwalteten Einstellungen

In vielen Konfigurationen funktioniert das Arbeiten mit verwalteten Einstellungen (MCX) nicht mehr zuverlässig. Das kann sich in folgenden Symptomen äußern:

- Das Anmelden von lokalen Benutzern an Clients (von Benutzern, die keine netzweiten Konten im Verzeichnisdienst besitzen), funktioniert möglicherweise nur mit großen Verzögerungen und erzeugt zahlreiche Fehlermeldungen im Konsolprotokoll.
- Bestimmte Einstellungen funktionieren nicht oder fehlerhaft. Sind zum Beispiel Vorgaben für die Benutzung von Druckerwarteschlangen und Standarddrucker definiert, so kann es sein, dass sich diese Konfiguration auf den Clients in regelmäßigen Abständen dupliziert. Drucker werden mehrfach oder falsch eingerichtet.

2.7.4 Unterstützung klassischer Mac OS-Systeme

Die folgenden Funktionen, die für die Integrationen von klassischen Mac OS-Systemen in ein Netzwerk benötigt werden können, werden nicht mehr unterstützt:

- Der Kommunikation mit Mac OS-Dateidiensten, die nur AFP over AppleTalk unterstützen, ist nicht mehr möglich. Es muss zwingend AFP over TCP/IP eingesetzt werden.
- Das Programm Macintosh Manager zur Verwaltung von Mac OS-Systemen im Netz, wird nicht mehr unterstützt. Es ist noch lauffähig, falls Sie es bei einer Aktualisierungsinstallation aus einem Panther- oder Jaguar-System übernommen haben, gilt jedoch nicht mehr als unterstützte Komponente von Mac OS X Tiger.

2.7.5 Arbeiten mit einem zentralen Netzwerkordner für Schriftarten

Die Konfiguration eines zentralen Netzwerkordners für Schriftarten am Pfad

```
/Network/Library/Fonts
```

über einen AFP-Automount-Eintrag funktioniert nicht mehr zuverlässig. Die Clients können von folgenden Symptomen betroffen sein:

- Der Schriftverwaltungsprozess von Mac OS X (ATSServer) kann beim Systemstart oder bei der Anmeldung in eine Endlosschleife geraten, was ein Einfrieren des Systems zur Folge hat.

- Es kann passieren, dass die Clients in unregelmäßigen Abständen sämtliche Netzwerkschriften aktivieren, auch wenn diese Schriften explizit von den Benutzern deaktiviert wurden. Da hierbei der komplette Zeichensatz-Cache neu aufgebaut werden muss, können sich beim Anmelden am Client-Rechner Verzögerungen von mehreren Minuten ergeben, bis das System wieder reagiert. Das unerwartete Aktivieren einer großen Anzahl von Schriften kann zudem weitere Verzögerungen und Fehlfunktionen in Carbon-Programmen auslösen.

2.7.6 Anbindung an NIS-Verzeichnisdienste

Die Anbindung an einen NIS-Verzeichnisdienst ist im Moment von kritischen Fehlern betroffen, so dass dringend davon abgeraten werden muss, Mac OS X 10.4 bereits jetzt in einem Netzwerk mit einem NIS-Verzeichnisdienst einzusetzen. Verwenden Sie ein heterogenes Unix-Netz, das auf die Verwendung von NFS und NIS ausgerichtet ist, so muss Tiger zurzeit als unbrauchbar bezeichnet werden.

Es gibt ernst zu nehmende Anzeichen dafür, dass ab Version 10.4.3 das System wieder im Zusammenhang mit NIS verwendbar wird. Ebenso gibt es Anzeichen dafür, dass Apple ab 10.4.3 auch die Verschlüsselung von Kennworten nach dem Verfahren *MD5* bei der Verwendung von NIS unterstützen wird (siehe Abschnitt 7.4.3 des Hauptbuchs). Dies erhöht die Kompatibilität mit modernen Unix-System deutlich.

2.7.7 Drucken im Netz

Die Übernahme einer früheren zentralen Druckserverkonfiguration in Tiger kann zu erheblichen Problemen, bis hin zu einem Totalausfall aller Netzwerkdruckfunktionen führen. In diesem Fall ist die einfachste Lösung, die Definitionen aller Druckerwarteschlangen auf dem Server komplett zu löschen und neu einzurichten. Verwenden Sie in diesem Fall bevorzugt das Protokoll IPP und lassen Sie die Clients die Drucker über Bonjour automatisch erkennen.

2.7.8 Faxempfangsserver und Faxempfang auf Clients

Apple hat das in Mac OS X enthaltene Telefaxprogramm auf eine Version aktualisiert, die mit dem Rest des Systems nicht mehr vollständig kompatibel ist. Als Folge davon ist der Absender eingehender Telefaxsendungen nicht mehr sichtbar und wird vom System nicht mehr richtig verarbeitet. Bei der Weiterleitung der Faxsendung per E-Mail werden alle Sendungen mit dem Vermerk

FAX from Unknown.pdf

versehen. Besonders beim Betrieb als Faxeingangsserver kann die Zuordnung der eingehenden Sendungen an einen Endempfänger daher nicht mehr automatisiert

erfolgen, sondern muss manuell durchgeführt werden.

2.7.9 Automatische Proxy-Konfiguration auf Clients

Die automatische Konfiguration von Proxy-Servern über eine *PAC-Datei*, die per HTTP zur Verfügung gestellt wird, ist in den ersten Versionen von Mac OS X Tiger nicht mehr möglich, da hierdurch auf den Clients Safari extrem instabil wird und sich so nicht mehr benutzen lässt. Als Abhilfe können Sie entweder einen anderen Web-Browser verwenden oder eine manuelle Konfiguration auf allen Clients vornehmen. Die explizite Konfiguration von Proxy-Servern ohne PAC-Datei funktioniert.

2.7.10 Verwendung von squid

Die im Buch vorgeschlagene Verwendung des freien Proxy-Servers *squid* ist noch möglich. Bei einer Übernahme der Konfiguration im Zusammenhang mit einer Aktualisierungsinstallation von Mac OS X 10.4 Server ist jedoch zu beachten, dass das System möglicherweise die Sicherheitseinstellungen der Startskripte bemängelt und deshalb squid nicht mehr automatisch startet. Sie können das Problem lösen, indem Sie die Einstellungen von Hand z.B. mit

```
sudo chown -R root:wheel /System/Library/squid
sudo chown -R root:wheel /System/Library/dansguardian
sudo chmod -R go-w /System/Library/squid
sudo chmod -R go-w /System/Library/dansguardian
```

anpassen.

2.7.11 Verwendung der NetBoot-Funktionen

Bestimmte Versionen von Mac OS X 10.4 Server führen zum Totalausfall der NetBoot-Funktionen. Stellen Sie sicher, dass Sie auf dem Server mindestens Version 10.4.2 einsetzen.

Kapitel 3

Installation eines Mac OS X-Netzes

3.1 Installationsplanung

Im großen und ganzen verläuft die Installation eines Netzes auf Basis mindestens eines Serversystems der Version 10.4 ähnlich wie schon unter 10.3, so dass dem Installations- und Planungskapitel nicht viel hinzuzufügen ist. Das deutsche Installationshandbuch inklusive Arbeitsblättern zum Notieren der Konfigurationsdaten liefert Apple nun auch bereits bei den ersten in Deutschland ausgelieferten Serverpaketen mit. Seit Juni 2005 stehen auch die auf 10.4 aktualisierten Handbücher mit insgesamt 17 Bänden unter der bekannten Adresse

```
http://www.apple.com/de/server/documentation/
```

als PDF-Downloads zur Verfügung.

Es sei an dieser Stelle nochmals darauf hingewiesen, dass das Vorhandensein eines korrekt funktionierenden und richtig konfigurierten DNS-Servers ganz entscheidend dafür ist, ein Mac OS X-Serversystem einwandfrei installieren zu können. Diese zwingende Voraussetzung hat sich in der Tiger-Version noch verschärft, da noch mehr Dienste kerberisiert sind. Planen Sie, den Server als neuen Zentralrechner zum Aufbau eines Netzwerks einzusetzen, so dass in der Regel der Einsatz des Rechners als Open Directory Master und Kerberos-Schlüsselverteilungsserver erforderlich ist, so ist dies von entscheidender Wichtigkeit. Die DNS-Domain des Server-Computers (genauer gesagt der Domain-Name zur IP-Adresse seines primären Netzwerkanschlusses) muss vor der Installation richtig eingerichtet sein, da sich hieraus indirekt während der Installation der Name des Kerberos-Bereichs (Realm-Name) und der Distinguished Name des LDAP-Suchpfades ergibt. Diese Werte nach der Installation noch zu ändern, erfordert ganz erhebliche Systemkenntnisse und könnte einige Probleme nach sich ziehen.

Stellen Sie daher unbedingt sicher, dass ein DNS-Server für Ihr eigenes Netzwerk korrekt läuft und auch der DNS-Domain-Name für Ihr privates Netz richtig und endgültig eingerichtet ist. Sollten Sie noch keinen eigenen DNS-Server haben, sondern soll der gerade zu installierende Mac OS X Server zum DNS-Server werden, so müssen Sie die Installation in folgenden Schritten durchführen:

1. Stellen Sie bei der Installation die Konfiguration des primären Netzwerkanschlusses auf MANUELL und geben Sie IP-Adresse und Domain-Name von Hand ein. Lassen Sie den Eintrag für DNS-SERVER zunächst weg.
2. Stellen Sie sicher, dass während dieser Installation der Rechner noch nicht als Open Directory Master konfiguriert wird. Dies würde sonst dazu führen, dass der Rechner seinen Bonjour-Namen fälschlicherweise als Basisname für den LDAP-Suchpfad und den Kerberos-Bereichsnamen heranzieht. Stellen Sie beim Konfigurationsschritt VERZEICHNISNUTZUNG zunächst die Betriebsart EIGENSTÄNDIGER SERVER ein.
3. Ist die Installation des Serverbetriebssystems beendet, richten Sie als Erstes den DNS-Dienst, falls gewünscht zusammen mit dem DHCP-Dienst, ein wie in Kapitel 3 des Buches beschrieben und testen Sie den Dienst intensiv auf korrekte Funktion. Der Server muss seinen eigenen vollständigen DNS-Namen, d.h. mitsamt seinem endgültigen DNS-Domainnamen korrekt ermitteln können.
4. Führen Sie dann mit dem Programm *Server Admin* eine Höherstufung der Betriebsart EIGENSTÄNDIGER SERVER auf die Betriebsart OPEN DIRECTORY MASTER durch. Nähere Hinweise siehe auch in Kapitel 9 des Hauptbuches.

Es sei nochmals daran erinnert, dass die Einrichtung eines Zeitsynchronisationsdienstes (auf Basis des NTP-Protokolls, wie von Apple vorgesehen und in Kapitel 3 des Hauptbuches beschrieben) für den Einsatz von Kerberos notwendig ist.

3.2 Einsatz von AppleTalk

Der Einsatz von *AppleTalk* ist wie im Hauptbuch beschrieben seit 1999 nicht mehr empfohlen. In den Tiger-Betriebssystemen hat Apple die Verwendungsmöglichkeiten für AppleTalk weiter eingeschränkt. AppleTalk ist nur noch zum Aufspüren von älteren Netzwerkdiensten *(Service Recovery)* verwendbar, die Verwendung als Transportprotokoll ist nun endgültig nicht mehr möglich. Sie können deshalb insbesondere *AppleShare over AppleTalk* zum Netzzugriff auf Dateien sehr alter Mac OS-Computer nicht mehr einsetzen. Läuft auf diesen Computern jedoch mindestens Mac OS 8, so können Sie diese auf *AppleShare over TCP/IP* umrüsten, indem Sie die Computer mindestens mit der Version 3.7 von AppleShare ausstatten und sie vom Datentransport über AppleTalk auf den Datentransport über TCP/IP umschalten. Aktualisierungen von AppleShare sind kostenlos über die Webseite

```
http://www.apple.com/support/
```

erhältlich. Auch falls Sie die folgenden Betriebssysteme in Ihrem Netzwerk einsetzen, prüfen Sie vor der Installation von Tiger-Clients oder -Servern unbedingt, ob dies nicht den Zugriff auf alte Dateiserverdienste versperren würde:

- Microsoft *Windows NT Server*, auf denen *Services for Macintosh* laufen
- Novell *NetWare* in Versionen vor 5.1
- Unix-Server mit *netatalk* in Versionen vor 1.4

3.3 Fernverwaltung eines Tiger-Servers

Wenn Sie aus organisatorischen Gründen einen 10.4-Server von einem anderen Arbeitsplatz aus ferneinrichten möchten oder müssen, z.B. weil der Server nicht mit einer Grafikkarte ausgestattet ist, stellen Sie sicher, dass Sie den Administratorrechner bereits unter Mac OS X 10.4 laufen haben und aktualisieren Sie dessen Software zur Fernadministration auf den Tiger-Releasestand. Die neueste Version der Software bleibt auch in der Tiger-Version mit den vorigen Serverversionen kompatibel. Sie können also damit wie bisher noch ältere Jaguar- und Panther-Server aus der Ferne verwalten.

Es empfiehlt sich, stets die neueste Version der Administratorprogramme von Apple herunter zu laden. Sie finden das Paket über die Adresse

```
http://www.apple.com/support/downloads/
```

unter dem Namen *Server Admin Tools 10.4*. Der *Macintosh Manager* zum Arbeiten mit verwalteten Einstellungen klassischer Mac OS-Rechner gehört nicht mehr zum Administrationspaket und wird unter Tiger nicht mehr offiziell unterstützt. Exemplare dieses Programms, die aus älteren Jaguar- und Panther-Servern übernommen wurden, laufen jedoch weiterhin.

3.4 Ablauf der Server-Installation

Die Dateigrößen der Installationspakete haben sich für Mac OS X 10.4 Server naturgemäß geändert. Tabelle 3.1 aktualisiert die Namen und die Größenangaben. Die Installation kann wahlweise von einer DVD oder von CD-ROMs erfolgen.

Richten Sie während der Installation den Servercomputer als Open Directory Master ein, so legt Tiger wie auch schon in Panther einen zusätzlichen Benutzer als Verwalter der Verzeichnisdienste an, der zum „initialen“ Benutzer in der Verzeichnisdatenbank wird. Dieses Benutzerkonto trägt jetzt nur einen neuen, vorgegebenen Namen, nämlich *diradmin*, und besitzt die UID 1000. Diese Technik macht auch unerfahrenen Netzverwaltern deutlicher, dass es sich bei dem Verwalter des Servercomputers und dem Verwalter der Verzeichnisdienste um zwei verschiedene

Paket	Paketgröße
Grundlegende Systemsoftware (erforderlich)	1,8 GB
Notwendige Serversoftware (erforderlich)	200 MB
Server-Administrations-Software (erforderlich)	72,9 MB
QuickTime Streaming Server (erforderlich)	37,2 MB
Software für Anwendungsserver (erforderlich)	198 MB
Sprachpaket deutsch	78,7 MB
Sprachpaket französisch	78 MB
Sprachpaket japanisch	81 MB
Brother-Druckertreiber	17,5 MB
Canon-Druckertreiber	345 MB
efi-Druckertreiber	58,1 MB
EPSON-Druckertreiber	652 MB
Gimp-Print-Druckertreiber	6,6 MB
Hewlett-Packard-Druckertreiber	257 MB
Lexmark-Druckertreiber	299 MB
Ricoh-Druckertreiber	944 KB
Xerox-Druckertreiber	15,7 MB
X11	90,8 MB
Xcode Tools	1,5 GB

Tabelle 3.1: Aktuelle Größen der Installationspakete von Mac OS X Server

Dinge handelt (siehe Seite 66 im Hauptbuch). Achten Sie wie bisher darauf, dass die während der Installation von Mac OS X angelegten Benutzerkonten alle mit dem gleichen Kennwort versehen werden. Dies betrifft

- den lokalen Verwalter des Servercomputers (Name wird vom Benutzer vorgegeben),
- den obersten Systemverwalter *root* (UID 0),
- und optional den Verzeichnisdienstverwalter *diradmin* (UID 1000), falls der Open Directory-Server aktiviert wird.

Nach der Installation können Sie die Kennworte dieser drei Konten auf unterschiedliche Werte setzen, falls erwünscht.

Es gibt verschiedene Konfigurationsschritte beim späteren Betrieb von Mac OS X Server, bei dem das Programm *Server Admin* nach einem Kennwort fragt, auch wenn Sie bereits als Administrator des jeweiligen Servers angemeldet sind. In diesem Fall handelt es sich meist um Konfigurationsschritte, die die Eingabe von Name und Kennwort des Verzeichnisdienstverwalters erfordern. Doch Vorsicht: Server Admin füllt das Dialogfenster zur nachträglichen Authentifizierung in vielen Fällen *mit dem Benutzernamen des Serververwalters aus* anstatt nach einer Anmeldung für den Verzeichnisdienstverwalter zu fragen. Dies kann zu verwirrenden Situationen

führen. Melden Sie sich mit einem „falschen“ der drei Verwalterkonten an, schlägt der laufende Konfigurationsvorgang mit irreführenden Meldungen fehl.

Bei der Ersteinrichtung von Serverdiensten während der Installation können Sie in Tiger die folgenden neuen Dienste zusätzlich auswählen:

- Apple Remote Desktop
- iChat-Server
- Software-Aktualisierungsserver
- WebDAV-Dateiserver
- Weblog-Server
- Xgrid Agent
- Xgrid Controller

Hierbei sind Apple Remote Desktop und der WebDAV-Dateiserver nicht wirklich neu, aber Sie können nun zu einem früheren Zeitpunkt wählen, ob Sie diese Dienste als Option einschalten möchten. Die hier genannten neuen Dienste können auch zu einem späteren Zeitpunkt noch aktiviert werden, die Auswahl, die Sie hier treffen, bestimmt nur, ob diese Dienste sofort „erstkonfiguriert“ und beim nächsten Start des Servers automatisch mitgestartet werden.

Kapitel 4

Einrichten der Netzinfrastruktur

4.1 Der DNS-Dienst

4.1.1 Neuerungen im weltweiten DNS-Betrieb

Zu den im Hauptbuch genannten DNS-Namen der obersten Ebene, die nicht länderbezogen sind, den *gTLDs (Generic Top Level Domains)*, haben sich inzwischen zwei neue Einträge gesellt, nämlich *jobs* und *travel*. Tabelle 4.1 zeigt die aktualisierte Gesamtübersicht.

4.1.2 Einrichtung eines DNS-Servers

Die von Apple in Tiger verwendete Version des DNS-Servers BIND ist die gleiche wie auch schon in 10.3, nämlich die Fassung 9.2.2. Von daher ergeben sich keine grundsätzlichen Änderungen für die Konfiguration des Servers auf der Kommandozeile. Für die Verwaltung von BIND über ein Fremdprogramm, wie das grafische *Server Admin* hat Apple jedoch die Sicherheitseinstellungen leicht erhöht. Wenn Sie einen frühere, von Hand angepasste DNS-Server-Konfiguration aus Panther übernehmen, stellen Sie bitte sicher, dass die Steuerungsoptionen von BIND richtig eingestellt sind. Damit die Steuerung über Server Admin richtig funktioniert, müssen mindestens die folgenden beiden Optionen in der Rubrik *controls* der Konfigurationsdatei */etc/named.conf* eingetragen sein:

```
include "/etc/rndc.key";
controls {
       inet 127.0.0.1 port 54 allow {any;}
       keys { "rndc-key"; };
};
```

Name	Beabsichtigte Nutzung
aero	Luftfahrtindustrie *(aeronautical)*
biz	Firmen, zur Ergänzung der überfüllten com-Domain *(business)*
com	Firmen *(commercial)*
coop	Verbände *(cooperative associations)*
edu	Bildungseinrichtungen der Vereinigten Staaten von Amerika *(educational)*
gov	Behörden der Vereinigten Staaten von Amerika *(governmental)*
info	Domain für „Sonstiges“ *(informational)*
int	durch Staatsverträge geschaffene internationale Organisationen *(international)*
jobs	Arbeitsvermittlung *(jobs)*
mil	militärische Einrichtungen der Vereinigten Staaten von Amerika *(military)*
museum	Museen *(museum)*
name	Privatleute *(names)*
net	Einrichtungen der Netzwerkinfrastruktur *(network)*
org	Gemeinnützige Organisationen *(non-profit organizations)*
pro	Zulassungspflichtige Berufe wie z.B. Ärzte *(credentialed professionals)*
travel	Tourismusindustrie *(travel)*

Tabelle 4.1: Aktuelle Liste der nicht länderbezogenen Domain-Namen der obersten Ebene

Diese Einstellungen bewirken, dass von einem Prozess des Servercomputers aus das laufende BIND-Programm gesteuert werden darf und dass Standardeinstellungen für eventuelle verschlüsselte Kommunikation auf dieser Steuerverbindung genutzt werden sollen.

Arbeiten mit den Konfigurationsdateien

Apple stellt in Tiger eine komplett überarbeitete grafische Oberfläche für die Einrichtung von DNS-Einträgen zur Verfügung und die meisten Mängel aus Panther sind behoben. Die Vorgehensweise wird im nächsten Abschnitt beschrieben. Konfigurieren Sie den DNS-Dienst jedoch in der Standardversion von Mac OS X oder verwenden Sie weitergehende Konfigurationsmöglichkeiten von BIND, so reicht die grafische Oberfläche nicht aus. Sie müssen in diesem Fall direkt auf den Konfigurationsdateien, nämlich */etc/named* und den Dateien im Ordner */var/named* arbeiten.

Hierzu zählt auch die Einrichtung eines privaten DNS-Servers, der vom offiziellen Internet aus nicht erreichbar ist, also eine *Forwarder*-Konfiguration, wie in Abschnitt 3.2.7 des Hauptbuches beschrieben. Bei der Einrichtung der Forwarder-Einträge ändert sich diesbezüglich in Tiger nichts.

Richten Sie eine neue DNS-Konfiguration ein, so ist es kein Problem, die Arbeit zwischen grafischer Oberfläche und der Arbeit auf der Kommandozeile aufzuteilen. Sie erstellen zunächst eine Basiskonfiguration mit Server Admin, wobei Sie die bequemen Einstellmöglichkeiten im Konfigurationsprogramm nutzen und wechseln danach für alle fortgeschrittenen Einstellmöglichkeiten auf die Kommandozeile.

Computerkurzname	Voller Name (FQDN)	IPv4-Adresse
g4server smtp pop nameserver	g4server.example.private smtp.example.private pop.example.private nameserver.example.private	192.168.1.1
alpha	alpha.example.private	192.168.1.2
beta	beta.example.private	192.168.1.3
router	router.example.private	192.168.1.4

Tabelle 4.2: Die Ausgangsdaten für ein kleines Beispielnetz

Konfiguration über das Server Admin-Programm

Um Ihnen den Umgang mit dem stark überarbeiteten DNS-Teil des Server Admin-Programms zu erläutern, zeigen wir Ihnen nachfolgend die Konfiguration am Beispiel eines kleinen Privatnetzes. Wir verwenden dazu das Beispiel aus dem Hauptbuch, das in Tabelle 4.2 noch einmal in leicht veränderter Form wiedergegeben ist. BIND soll hierbei auf dem Mac OS X 10.4 Server mit dem DNS-Namen *g4server* in der Domain *example.private* laufen.

1. Starten Sie *Server Admin* und stellen Sie die Verbindung mit dem Server her, auf dem der DNS-Dienst eingerichtet werden soll.
2. Wählen Sie in der Übersicht COMPUTER & DIENSTE den Punkt DNS und öffnen Sie dort die Rubrik EINSTELLUNGEN.
3. Stellen Sie auf der Karteikarte ALLGEMEIN die gewünschte Betriebsart des DNS-Servers ein, wie in Abschnitt 3.2.4 des Hauptbuchs beschrieben.
4. Wechseln Sie zur Karteikarte ZONEN und betätigen Sie die Schalfläche + unterhalb der Tabelle. Wir richten den Server für die Zone *example.private* ein.
5. Geben Sie in das Feld ZONENNAME den DNS-Namen der Domain ein. In unserem Beispiel würde er *example.private* lauten. Ein abschließender Punkt nach dem Namen zur Kennzeichnung der obersten DNS-Namensebene ist an dieser Stelle nicht erforderlich.
6. Geben Sie in das Feld SERVERNAME den Kurznamen des Servers ein, den Sie gerade konfigurieren. Sie sollten in diesem Fall den „Rufnamen“ des Servers, keinen institutionellen Aliasnamen verwenden. In unserem Beispiel lautet der richtige Eintrag *g4server*.
7. Stellen Sie sicher, dass bei SERVER-IP-ADRESSE die richtige primäre Adresse des lokalen Servers eingestellt ist. Normalerweise muss hier nichts verändert werden.
8. Stellen Sie bei ADMINISTRATOR-MAIL die Mailadresse der Person ein, die diesen DNS-Server verwaltet.

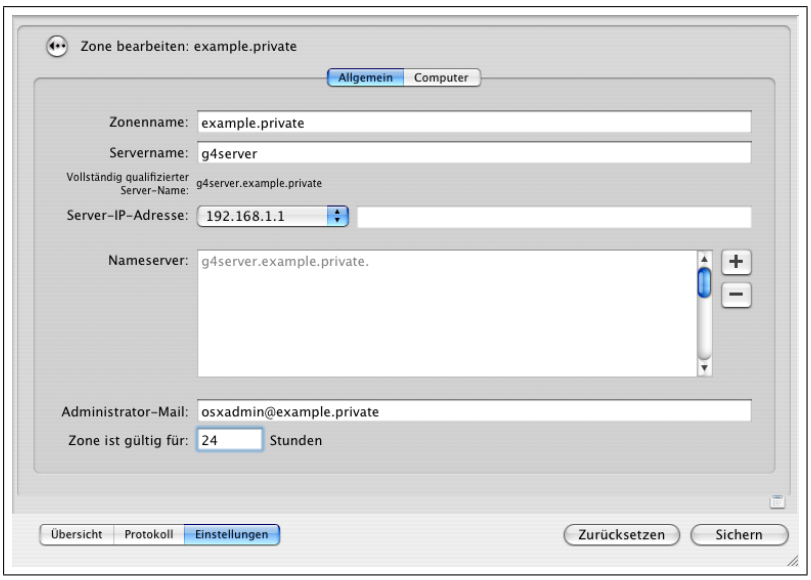

Abbildung 4.1: Einrichtung einer neuen Zone über Server Admin

9. Geben Sie bei ZONE IST GÜLTIG FÜR die Standardlebensdauer bis zur nächsten Wiederauffrischung der Zonendaten ein. Sie können den Standardwert von 24 Stunden übernehmen.

10. Betätigen Sie die Schaltfläche SICHERN rechts unten im Fenster. Abbildung 4.1 fasst noch einmal die eingetragenen Werte zusammen.

Durch diesen ersten Schritt richtet Mac OS X die Konfigurationsdatei */etc/named* und die beiden Zonendateien für Vor- und Rückwärtsauflösung unter */var/named* ein, in unserem Beispiel mit den Namen

```
/var/named/example.private.zone
/var/named/db.192.168.1
```

Als nächstes richten wir die institutionellen Aliasnamen für unseren Server ein und füllen die Beschreibungsfelder aus. Gleichzeitig markieren wir den Server als Mail-Server für unsere Domain. Server Admin erstellt für uns automatisch die nötigen CNAME-, TXT- und MX-Einträge.

1. Wechseln Sie zur Karteikarte COMPUTER. (Sie befinden sich immer noch in der Zonenkonfiguration *example.private*.)

2. Doppelklicken Sie den ersten erstellten Eintrag, in unserem Beispiel *g4server*.

3. Das Konfigurationsblatt zum Einrichten eines Adresseintrags öffnet sich. Betätigen Sie neben dem Feld ALIASE den Plus-Knopf.

4. Geben Sie an das neu erscheinende Feld den Aliasnamen, in unserem Beispiel *smtp* ein.
5. Wiederholen Sie die letzten beiden Schritte für die Aliasnamen *pop* und *nameserver*.
6. Kreuzen Sie das Feld IST EIN MAIL-SERVER FÜR DIE ZONE an. Geben Sie als Priorität den Standardwert 10 ein.
7. Geben Sie auf Wunsch Beschreibungstexte in die Felder HARDWARE-INFO, SOFTWARE-INFO und KOMMENTAR und drücken Sie OK. Beachten Sie diesbezüglich die Sicherheitshinweise im Hauptbuch. Wenn es sich um ein abgeschlossenes privates Netz handelt, können diese Einträge die Wartungsfreundlichkeit erhöhen. Wenn es sich um einen Server handelt, auf den vom Internet aus zugegriffen werden kann, machen Sie den Server angreifbarer, wenn Sie zu viele technische Informationen öffentlich preisgeben.

Abbildung 4.2 zeigt den fertigen Eintrag. Drücken Sie nun die Plus-Schaltfläche unterhalb der Computertabelle, um die Einträge für die anderen Computer unseres Beispielnetzes anzulegen. In diesem Fall reicht es, in das Konfigurationsformular nur die Einträge IP-ADRESSE und NAME und – falls Sie dies nutzen möchten – die Felder HARDWARE-INFO, SOFTWARE-INFO und KOMMENTAR auszufüllen. Für unser Beispielnetz erhalten wir schließlich die Tabelle in Abbildung 4.3. Sie können die Konfiguration mit dem Knopf SICHERN abspeichern und den DNS-Dienst mit dem Knopf in der Symbolleiste starten.

4.1.3 Einrichtung eines DHCP-Servers

Bezüglich der Einrichtung des DHCP-Servers verhält es sich in Tiger ähnlich wie bei BIND: Der Unterbau ist gleich geblieben, jedoch stellt die grafische Oberfläche von Server Admin zusätzliche Möglichkeiten zur Verfügung. Neu hinzugekommen ist die Möglichkeit, statische Adressen für die DHCP-Vergabe nun direkt eingeben zu können, ohne die NetInfo-Datenbank manipulieren zu müssen. Sie können Kapitel 3.3.2 des Hauptbuches nun durch folgende Vorgehensweise ersetzen:

1. Starten Sie *Server Admin* und stellen Sie die Verbindung mit dem DHCP-Server her, auf dem Sie statische Adresszuordnungen einrichten wollen.
2. Wählen Sie in der Übersicht COMPUTER & DIENSTE den Dienst DHCP aus.
3. Wählen Sie die Rubrik EINSTELLUNGEN und dort die Rubrik STATISCHE ZUORDNUNGEN.
4. Durch Drücken der Plus-Schaltfläche unterhalb der Tabelle können Sie einen neuen Eintrag anlegen. Es erscheint ein Eingabeformular.
5. Geben Sie in das Feld ETHERNETADRESSE die MAC-Adresse des Ethernet-, Firewire- oder WLAN-Anschlusses ein, auf dem Sie eine statische Adresszuordnung vornehmen möchten.

Abbildung 4.2: Eintrag für unseren Beispielserver, der neben anderen Aufgaben als DNS- und Mailserver arbeiten soll

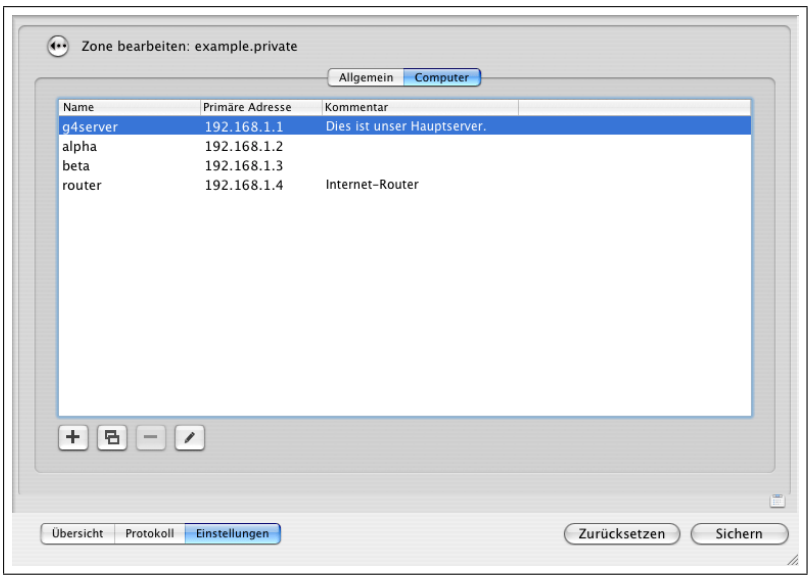

Abbildung 4.3: Das Beispielnetz beschränkt sich auf wenige Einträge.

6. Geben Sie in das Feld IP-ADRESSE die statische Adresse im IPv4-Format ein.
7. Geben Sie in das Feld BESCHREIBUNG den DNS-Kurznamen des jeweiligen Computers ein und drücken Sie auf OK.
8. Sind alle gewünschten Adresszuordnungen eintragen, betätigen Sie die Schaltfläche SICHERN in der unteren rechten Ecke des Fensters.

Abbildung 4.4 zeigt ein Beispiel eines Einzeleintrags, Abbildung 4.5 eine ganze Tabelle von Rechnern.

Eine Falle ist das Feld BESCHREIBUNG des DHCP-Eintrags. Apples Beschriftung suggeriert, es würde sich hier um ein Bemerkungsfeld handeln, in dem Sie z.B. den Rechnertyp beschreiben können. Dies ist jedoch nicht der Fall! Es handelt sich in Wirklichkeit um den Namen, mit dem der DHCP-Server den fertigen Eintrag in der NetInfo-Datenbank abspeichert. Dieser Name muss eindeutig sein. Haben Sie beispielsweise mehrmals den Begriff *PowerBook* in neu angelegte Beschreibungen eingetragen, werden Sie beim Drücken der Taste SICHERN eine böse Überraschung erleben: Server Admin löscht in diesem Fall ohne Vorwarnung alle Einträge mit doppelten Vorkommen des Wortes *PowerBook*, also alle Datensätze, die einen gleichen Inhalt im Feld BESCHREIBUNG aufweisen. Sie müssen alle betroffenen Einträge wieder neu eingeben.
Sie sollten daher in dieses Feld keine Beschreibung, sondern den DNS-Kurznamen der jeweiligen IP-Adresse eintragen.

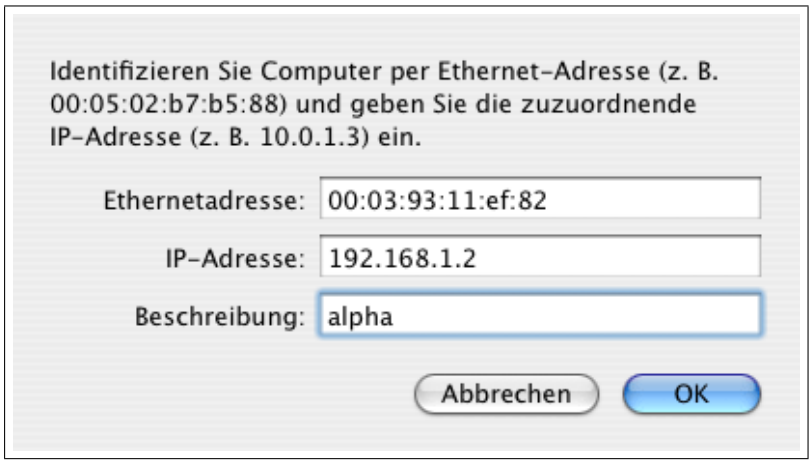

Abbildung 4.4: Beispiel für einen statischen Adresseintrag im DHCP-Server

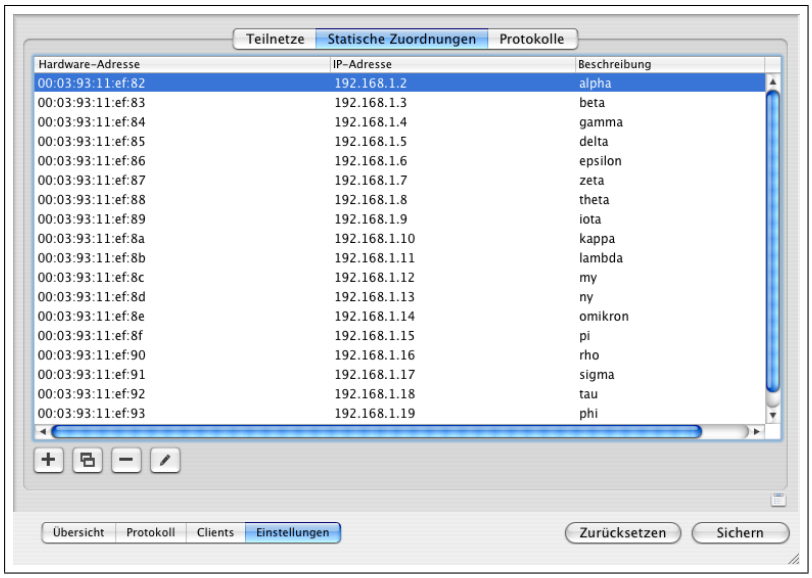

Abbildung 4.5: Es können beliebig viele statische Adressen für den DHCP-Server eingerichtet werden. Achten Sie darauf, dass die Eintragungen in der dritten Spalte eindeutig sind.

Kapitel 5

Das Berechtigungskonzept in Mac OS X

5.1 Die neue Technik: Zugriffssteuerungslisten

Mit den sogenannten *Zugriffssteuerungslisten*, auf englisch *Access Control Lists (ACLs)* genannt, führt Apple neben den klassischen POSIX-Berechtigungen eine zusätzliche Methode für die Vergabe von Benutzerrechten ein. Diese stellen eine Ergänzung der bisherigen Technik dar und lassen sich nicht nur auf Dateisystemobjekte wie Dateien und Ordner anwenden, sondern sie können auch für bestimmte Netzwerkdienste eingesetzt werden.

Apple verwendet ACLs in einer Form, die auch mit anderen Unix-Systemen sowie mit allen neueren Windows-Systemen (Windows NT, Windows XP, Windows 2003 Server) kompatibel ist. Zur Erinnerung: Die klassischen POSIX-Berechtigungen basieren auf den folgenden Prinzipien:

- Für jedes Dateisystemobjekt (Datei oder Ordner) wird über einen Satz von Attributen das Zugriffsrecht auf dieses Objekt definiert.

- Es gibt immer drei Parteien, für die man Zugriffsprivilegien definieren kann: Rechte für den **Eigentümer** des Objekts, Rechte für eine **Benutzergruppe** und Rechte für **Jeden**. Der Begriff „Jeder" schließt hier wirklich den kompletten Rest der Welt ein, also alle Personen, die auf irgendeine Weise Zugriff auf den betreffenden Computer erlangen, egal ob sie sich dafür identifizieren müssen oder nicht.

- Für jede Partei lassen sich Rechte für die Operationen **Lesen**, **Schreiben** und **Ausführen** vergeben. Mit „Ausführen" ist bei Dateien das Starten eines Programms, das sich in dieser Datei befindet, gemeint, bei Ordnern das Auflisten des Ordnerinhalts.

Hinzu kommen eventuelle Sonderrechte, wie die SUID-, SGID- oder Sticky-Markierungen, die im Hauptbuch detailliert erläutert werden. Zwar haben sich diese Unix/POSIX-Berechtigungen in den letzten 30 Jahren sehr gut bewährt, jedoch gibt es einige kleine Nachteile, die man versucht, mit den ACLs zu umgehen. Hierzu gehört beispielsweise das Problem, das man in der Praxis Fälle hat, in denen man auch das Zugriffsrecht auf die Rechte selbst steuern möchte. Dies ist mit der herkömmlichen Methode nicht möglich, denn das Recht, Zugriffsattribute verändern zu dürfen, ist an das Schreibrecht auf den umschließenden Ordner gekoppelt. Eine feinere Möglichkeit, dies einstellen und abstimmen zu können, ist nicht möglich.

Ebenso ist in der Praxis oft die „Allmacht" des root-Benutzers ein Problem: Das Benutzerkonto *root* definiert einen speziell ausgezeichneten Benutzer, der das Recht hat, *alle* Zugriffsattribute beliebig ändern zu dürfen. In Firmen gehört das root-Benutzerkonto üblicherweise einem oder mehreren Mitarbeitern der IT-Abteilung. Auch wenn das root-Konto niemals zur normalen Arbeit genutzt wird, kann dies ein Datenschutzproblem darstellen, denn auf diese Weise hat diese Abteilung grundsätzlich Zugriff auf alle Informationen, die auf allen Computern gespeichert sind, zum Beispiel auch auf personenbezogene, vertrauliche Personaldaten, die von Gesetz wegen besonders geschützt sein müssten. Mit ACLs lassen sich solche Probleme lösen, indem die Rechte feiner abgestimmt, auf mehr als drei Parteien verteilt und auch Zugriffsverbote definiert werden können.

5.2 ACLs im Detail

5.2.1 GUIDs und ihre Anwendung

Eine Zugriffssteuerungsliste *ergänzt* die herkömmlichen POSIX-Rechte. Sie sind also nicht gezwungen, mit ACLs zu arbeiten. Die bisherige Rechtevergabe gilt auch weiterhin noch, sie wird nur durch neue Regeln erweitert. Technisch gesehen sind ACLs über Listen realisiert, die an die einzelnen Dateisystemobjekte geknüpft werden können. Eine ACL kann entweder leer sein – dann gelten nur die POSIX-Rechte wie bisher – oder sie enthält einen, bzw. beliebig viele *Zugriffssteuerungseinträge (Access Control Entries, ACEs)*. In einem solchen Eintrag ist verzeichnet,

- *für wen* dieser Eintrag gilt (z.B. für einen bestimmten Benutzer oder eine Benutzergruppe),
- ob es sich um ein *Zugriffsrecht* oder *Zugriffsverbot* handelt,
- um welches *Recht* es im Detail geht und
- wie dieses Recht in einer Hierarchie von Ordnern an Ordner tiefer in der Hierarchie *vererbt* werden soll, bzw. ob es sich bei diesem Eintrag um ein geerbten Eintrag handelt.

Beginnen wir mit dem ersten Punkt: Mac OS X speichert die Information, welcher Benutzer oder welche Benutzergruppe ein bestimmtes Recht besitzt, über ei-

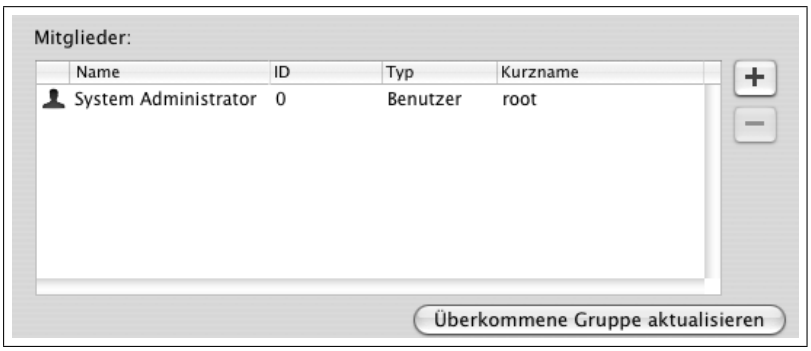

Abbildung 5.1: Eine oder mehrere Gruppen, die Sie aus früheren Mac OS X-Versionen übernommen haben, können mit dem Knopf rechts unten auf die Verwendung von GUIDs aktualisiert werden.

ne *GUID (Globally Unique Identifier, global eindeutiger Bezeichner)* ab. In früheren Versionen von Mac OS X hat Apple diese Identifikation auch *Generated Unique Identifier (erzeugter eindeutiger Bezeichner)* genannt. In der deutschen Fachsprache ist sowohl die Sprechweise „der GUID" als auch „die GUID" geläufig. GUIDs sind eindeutige Schlüsselnummern mit 128 Bit Länge. Sie werden in der Form

```
19ADB10A-4471-11D8-9B71-000393C0ECE6
```

geschrieben, also als hexadezimale Zahlenfolge, die mit Bindestrichen in fünf Teile mit jeweils vier, zwei, zwei, zwei und sechs Byte unterteilt ist. Mac OS X verwendet ein spezielles Verfahren zum Erzeugen solcher GUIDs, das es so gut wie unmöglich macht, dass zwei jemals erzeugte GUIDs zufällig gleich sein können. Für alle Objekte dieser Welt, die verschieden sind, werden also unterschiedliche GUIDs verwendet. GUIDs entsprechen ungefähr den SIDs aus der Windows-Welt (siehe Hauptbuch), werden jedoch anders notiert.

Seit Mac OS X 10.2 sind die Konten aller Benutzer bereits mit solchen GUIDs versehen, verwendet werden sie jedoch erst ab Mac OS X 10.4. Für Konten von Benutzergruppen gilt das nicht. Wenn Sie ein System von einer früheren Version auf Mac OS X Tiger aktualisieren, sollten Sie deshalb nach der Installation alle Benutzergruppen, die später ACLs verwenden dürfen, mit GUIDs versehen. Dies geschieht, indem Sie im Arbeitsgruppen-Manager die betreffende Benutzergruppe auswählen und den rechts unten erscheinenden Knopf ÜBERKOMMENE GRUPPE AKTUALISIEREN drücken (Abbildung 5.1).

Hierbei werden auch die Verweise auf die Gruppenmitglieder aktualisiert. Die Mitglieder werden also nicht mehr nur per Kurznamensnennung, sondern intern auch per GUID-Verweis gespeichert. Da sowohl Benutzer als auch Gruppen sich über GUIDs identifizieren lassen, können auch Gruppen als Mitglieder einer Gruppe auftreten. Mit anderen Worten: Es ist jetzt durchaus erlaubt, verschachtelte Gruppen anzulegen. Sie können also eine Benutzergruppe *Angestellte* anlegen, welche als Mitglieder die Gruppen *Buchhaltung*, *Marketing* und *Personalabteilung* enthält.

Um sich die GUIDs anzeigen zu lassen, stellen Sie sicher, dass die Detailansicht im Arbeitsgruppen-Manager aktiviert ist. Sie können dies über den Menüpunkt ARBEITSGRUPPEN-MANAGER | EINSTELLUNGEN durch Ankreuzen des Felds TITEL „ALLE EINTRÄGE“ UND „DETAILANSICHT EINBLENDEN“ bewirken. In der Detailansicht der jeweiligen Objekte sind die GUIDs nun unter dem Namen *GeneratedUID*, bzw. dem Open Directory-Rohnamen *dsAttrTypeNative:apple-generateduid* sichtbar.

Der zweite Punkt eines Zugriffssteuerungseintrags, nämlich ob es sich um ein Recht oder ein Verbot handelt, ist recht schnell abgehandelt: Mac OS X speichert entweder die Markierung *Erlauben* oder die Markierung *Ablehnen* im ACE ab.

5.2.2 Zugriffsoperationen

Kommen wir zum dritten Punkt, der Art des Zugriffs, für die ein Recht erteilt oder verweigert werden soll. Mac OS X unterstützt insgesamt 13 verschiedene Operationen, für die eine Berechtigung definiert werden kann:

- **Daten lesen:** Das Recht, den Inhalt einer Datei zu lesen, oder den Inhalt eines Ordners auflisten zu lassen.
- **Daten ausführen / durchqueren:** Das Recht, eine Datei als Programm ausführen zu können, beziehungsweise bei Ordnern, einen Unterordner zu öffnen.
- **Attribute lesen:** Das Recht, die Attribute zu einem Dateiobjekt, zum Beispiel Name, Erstellungsdatum und Größe zu lesen.
- **Erweiterte Attribute lesen:** Das Recht, weitere Zusatzdaten, die zu einer Datei gespeichert sein können, zu lesen. Mac OS X Tiger besitzt die Möglichkeit, Attribute, die von Programmen relativ frei definiert werden können, an Dateisystemobjekte anzuhängen. Solche Attribute werden zum Beispiel von *Spotlight* verwendet.
- **Zugriffsrechte lesen:** Das Recht, die Zugriffsrechte eines Dateiobjekts lesen zu dürfen.
- **Daten schreiben:** Das Recht, den Inhalt einer Datei zu schreiben und zu ändern; bei einem Ordner das Recht, eine Datei neu anzulegen.
- **Daten anhängen:** Das Recht, an eine Datei weitere Daten anzuhängen, bzw. bei einem Ordner das Recht, einen Unterordner neu anzulegen.
- **Attribute schreiben:** Das Recht, die Attribute eines Dateiobjekts, zum Beispiel das Erstellungsdatum, zu verändern.
- **Erweiterte Attribute schreiben:** Das Recht, zusätzliche, von einem Programm frei definierbare Attribute für ein Dateisystemobjekt anzulegen oder zu ändern.

- **Zugriffsrecht ändern:** Das Recht, ein Zugriffsrecht zu ändern.
- **Eigentümer ändern:** Das Recht, den Eigentümereintrag eines Dateisystemobjekts zu ändern. Dieses Recht ist zusätzlich so eingeschränkt, dass nur ein Rechteinhaber sich selbst zum Eigentümer machen kann. Es ist jedoch nicht möglich, jemand anders zum Eigentümer zu machen, also ein Objekt zu „verschenken".
- **Löschen:** Das Recht, dieses Dateisystemobjekt zu löschen.
- **Unterordner löschen:** Das Recht, einen Unterordner mitsamt den enthaltenen Dateien zu löschen.

5.2.3 Vererbung der Einträge in der Ordnerhierarchie

Der vierte Punkt eines Zugriffssteuerungseintrags betrifft die Vererbung von Zugriffsrechten auf Unterordner. Es gibt insgesamt vier Möglichkeiten:

- **auf diesen Ordner anwenden:** der Eintrag bezieht sich auf genau den Ordner, mit dem der Eintrag verknüpft ist.
- **auf unmittelbare Unterordner vererben:** der Eintrag wird auf Unterordner vererbt, die direkt in diesem Ordner enthalten sind (nicht auf Objekte weiter unten in der Hierarchie).
- **auf unmittelbar enthaltene Dateien vererben:** der Eintrag wird auf die direkt enthaltenen Dateien vererbt (nicht auf Dateien, die sich weiter unten in der Ordnerhierarchie befinden).
- **auf weiter unten enthaltene Objekte vererben:** der Eintrag wird auf weiter unten in der Hierarchie enthaltenen Ordner und Dateien vererbt (jedoch nicht auf Dateien und Ordner, die unmittelbar in diesem Ordner liegen)

Vorsicht: Sie müssen beachten, dass Sie diese vier Vererbungsmethoden kombinieren können, jedoch nicht in allen theoretisch denkbaren Kombinationen! Es gibt 12 von insgesamt 16 möglichen Kombinationen, die sinnvoll sind. Tabelle 5.1 erläutert dies noch einmal genauer. Führen Sie sich außerdem noch einmal vor Augen, dass es hier nicht um die direkte *Anwendung* von Rechten auf Dateisystemobjekte geht, sondern nur um die *Vererbung* der Rechte eines Ordners auf andere Objekte, die sich auf gleicher Höhe oder weiter unten in der Ordnerhierarchie befinden. Diese Vererbung findet nur dann statt, wenn entweder

- eine Datei oder ein Ordner in dieser Ordnerhierarchie neu angelegt wird,
- oder wenn mit einem Programm zum Einstellen von Dateirechten das Recht des obersten Ordners der Teilhierarchie geändert wird.

1	2	3	4	**Vererbung auf:**
–	–	–	–	überhaupt kein Objekt
●	–	–	–	diesen Ordner
–	●	–	–	nur direkt enthaltene Unterordner dieses Ordners
●	●	–	–	diesen Ordner und direkt enthaltene Unterordner
–	–	●	–	nur direkt in diesem Ordner enthaltene Dateien
●	–	●	–	diesen Ordner und direkt in diesem Ordner enthaltene Dateien
–	●	●	–	direkt enthaltene Objekte, jedoch nicht auf diesen Ordner
●	●	●	–	diesen Ordner und alle direkt enthaltenen Objekte
–	–	–	●	*nicht sinnvolle Kombination*
●	–	–	●	*nicht sinnvolle Kombination*
–	●	–	●	direkt enthaltene Ordner und deren Unterordner in beliebiger Tiefe
●	●	–	●	diesen Ordner und alle enthaltenen Ordner in beliebiger Tiefe
–	–	●	●	*nicht sinnvolle Kombination*
●	–	●	●	*nicht sinnvolle Kombination*
–	●	●	●	alle enthaltenen Objekte, jedoch nicht auf diesen Ordner
●	●	●	●	diesen Ordner und alle enthaltenen Objekte in beliebiger Tiefe

Tabelle 5.1: Zulässige Kombinationen der Vererbungsmethoden: (1) dieser Ordner, (2) unmittelbar enthaltene Ordner, (3) direkt enthaltene Dateien, (4) untergeordnete Objekte dieses Ordners auf tieferen Hierarchie-Ebenen

Wenn Sie nun später ein solches Objekt in der Hierarchie auswählen und dessen Zugriffsrechte erneut ändern, findet eine *Kombination* von Zugriffsrechten statt: Zum einen gibt es die Rechte, die dieses Objekt von einem übergeordneten Ordner ererbt haben kann, zum anderen gibt es Rechte, die Sie zusätzlich auf diesem Punkt der Ordnerhierarchie setzen. Mac OS X bezeichnet ersteres als *übernommene Zugriffsrechte*, letzteres als *explizite Zugriffsrechte*.

Hierbei kann es natürlich passieren, dass Sie einen von weiter oben in der Ordnerhierarchie übernommenen Zugriffssteuerungseintrag im aktuellen Objekt ändern möchten, z.B. weil Sie ein neues Recht vergeben möchten, das mit dem ererbten in Widerspruch steht. In diesem Fall müssen Sie zunächst für dieses Objekt eine *Umwandlung* von einem übernommenen in einen expliziten Zugriffssteuerungseintrag durchführen.

5.2.4 Auswertung der Zugriffssteuerungseinträge

Wie erwähnt kann eine Zugriffssteuerungsliste aus einer ganzen Reihe von Einträgen bestehen. Hierbei kann es leicht dazu kommen, dass zwei Einträge sich auf ein und dieselbe Zugriffspartei beziehen und sich ergänzen oder miteinander in Konflikt stehen. Z.B. könnten Sie gleichzeitig ein Recht für einen bestimmten Benutzer und ein Verbot für eine Gruppe, in der dieser Benutzer Mitglied ist, definieren. Damit es hier zu einer eindeutigen Regelung kommt, hält Mac OS X eine saubere Auswertungsreihenfolge ein, in der die Liste der Zugriffssteuerungseinträge abge-

arbeitet wird. Hierbei kommen folgende Grundsätze zur Anwendung:

- Soll eine Zugriffsoperation stattfinden, für die eine ACL-Berechtigung definiert werden kann, so geht Mac OS X die ACL von oben nach unten durch, um zu ermitteln, ob der Zugriff erlaubt ist oder abgelehnt werden muss. Die Liste wird hierbei immer bis zum Ende abgearbeitet und die Auswertung nicht vorher abgebrochen, sobald der erste „passende" Eintrag gefunden wird.
- Nach Auswertung der ACL werden zusätzlich die POSIX-Berechtigungen geprüft. (Ist die ACL leer, werden demzufolge ausschließlich die POSIX-Attribute getestet.)
- Die Einstellung *Ablehnen* hat immer Vorrang vor der Einstellung *Erlauben*. Findet Mac OS X einen zutreffenden Ablehnungseintrag, so wird der Zugriff verweigert, auch wenn zusätzliche Erlaubniseinträge für den Benutzer vorhanden sein sollten.
- Die Erlaubnis-Einträge ergänzen sich. Ist ein Benutzer beispielsweise Mitglied einer Gruppe, die Schreibrecht auf ein Objekt hat und Mitglied einer Gruppe, die Leserecht für ein Objekt hat, so hat dieser Benutzer am Ende Schreib- und Leserecht für dieses Objekt.

5.3 Wichtige Hinweise zum Einsatz von ACLs

5.3.1 Beschränkte Einsatzmöglichkeit

ACLs können nur im Zusammenhang mit solchen Dateisystemen verwendet werden, die die Speicherung und Auswertung von Zugriffssteuerungslisten für Dateisystemobjekte unterstützen. Im Moment werden nur drei Dateisysteme unterstützt:

- lokaler Zugriff auf ein Dateisystem im Format HFS+
- Netzwerkzugriff auf einen AFP-Dateiserver (AppleShare), der ACLs unterstützt
- Netzwerkzugriff auf einen CIFS/SMB-Dateiserver (Windows), der ACLs unterstützt

Die lokalen Dateisysteme UFS, DOS (FAT) oder NTFS, sowie der Fernzugriff über die Protokolle NFS, FTP und WebDAV sind also von der Nutzung von ACLs ausgeschlossen.

5.3.2 Anwendung der Zugriffssteuerung auf Dienste

Nicht nur Dateien und Ordner, sondern auch Dienste eines Tiger-Servers können mit ACLs versehen werden. Man spricht in diesem Fall von *SACLs* oder *Service Access Control Lists*. Im Moment ist die Vergabe dieser Berechtigungen auf die folgenden Dienste beschränkt:

- Anmeldung am Anmeldefenster von Mac OS X
- Zugriff auf den AFP-Dateiserver
- Zugriff auf den FTP-Server
- Zugriff auf den iChat-Serverdienst
- Zugriff auf die Mail-Serverdienste
- Zugriff über die ferne Kommandozeile *(Secure Shell, SSH)*
- Fernverbindung über einen VPN-Zugang
- Zugriff auf den Web-Server
- Zugriff auf Weblog-Funktionen
- Zugriff auf den CIFS/SMB-Dateiserver (Windows)
- Zugriff auf Xgrid-Funktionen

Die entsprechende Einstellung wird mit dem Programm *Server Admin* vorgenommen und weiter unten näher erläutert.

5.3.3 Ratschläge zur Verwendung

Aus den Ausführungen in den letzten Abschnitten ist ersichtlich geworden, dass ACLs Ihnen zwar wesentlich feiner abstimmbare Möglichkeiten eröffnen, Rechte für Objekte zu erteilen, jedoch gibt es so viele Möglichkeiten, dass dies zu einer komplexen Angelegenheit werden kann. Es gibt 13 Zugriffsarten und 12 mögliche Vererbungskombinationen, wodurch sich

$$2^{13} \cdot 12 = 98304$$

mögliche Einstellungen für einen Zugriffssteuerungseintrag ergeben. Dieser kann entweder als Erlaubnis oder Ablehnung definiert werden und sich auf eine beliebige im System vorhandene GUID beziehen. Der Eintrag ist Teil einer Liste mit beliebig vielen Einträgen und es besteht die Freiheit, jedes Dateisystemobjekt auf einem Volume mit unterschiedlichen Listen auszustatten. Die Wartung all dieser Einträge kann leicht zu einem Albtraum werden, wenn Sie es mit der Anwendung von ACLs übertreiben. Wenn Sie keine Erfahrung mit ACLs haben, kann es außerdem passieren, dass Sie aus Versehen ein Zugriffsverbot für eine Datei definieren, das von keinem Benutzer mehr geändert werden kann. Eine solche Datei lässt sich möglicherweise nie mehr löschen, es sei denn, Sie formatieren das komplette Volume neu oder schalten die ACL-Unterstützung für das Volume ab. Aus diesen Gründen sollten Sie ACLs nur mit äußerster Zurückhaltung einsetzen. Folgende Ratschläge sind sinnvoll:

- Verwenden Sie ACLs nur dann, wenn es unbedingt sein muss, d.h. wenn eine besondere Zugriffsberechtigung vorliegt, die sich mit den herkömmlichen POSIX-Einstellungen nicht mehr formulieren lässt. Wenn Sie in einem Netzwerk Vererbungsregeln für die Rechte beim Zugriff auf AFP- oder CIFS/SMB-Fileserver brauchen, so können Sie dies auch über eine Einstellung des File Servers ohne Verwendung von ACLs realisieren (siehe Abschnitt 6.5.3 im Hauptbuch).

- Definieren Sie so wenig Benutzergruppen wie möglich. Es sollte keine Überorganisation der Benutzer stattfinden, nur weil es möglich ist. Legen Sie eine Benutzergruppe immer dann an, wenn Sie in Ihrem Netz eine Gruppe von Benutzern ausmachen, denen gleiche Berechtigungen zugewiesen werden sollen.

- Vermeiden Sie es, Berechtigungen einzelnen Benutzerkonten zuzuweisen. Verwenden Sie stattdessen wann immer es geht Gruppenberechtigungen, so dass Sie über jede Gruppe jeweils einen bestimmten Typ von Zugriffsart definieren können. Es sollten sich einfache Regeln für diese Zugriffsklassen formulieren lassen, zum Beispiel „Nur die Gruppen *Buchhaltung* und *Administratoren* haben Schreibzugriff auf den Ordner /*Public*/*Buchhalt* und alle darin enthaltenen Objekte.“. Die Definition von Gruppen ermöglicht es, einer großen Zahl von Benutzern mit einem einzigen Mausklick ein Recht zu erteilen oder wegzunehmen, egal wie sich die Anzahl der Benutzer und die Anzahl der angelegten Unterordner entwickelt.

- Wenn Sie Daten vor Zugriff schützen müssen – wozu Sie im Einzelfall gesetzlich verpflichtet sein können –, so beginnen Sie mit einer stark eingeschränkten POSIX-Berechtigung (z.B. nur Schreib-/Leserecht für *root*, Gruppe *admin*) und fügen Sie nach und nach Gruppenerlaubniseinträge für die Gruppen hinzu, denen ein Recht erteilt werden soll.

- Nutzen Sie die Vererbungseinstellungen wann immer möglich. Die Vererbung ist eine effiziente Technik, eine große Zahl von Objekten automatisch mit den richtigen Berechtigungseinstellungen zu versehen. Durch Einstellen der richtigen Rechte von oben nach unten in der Ordnerhierarchie kommen Sie mit so wenig Einstellungen wie möglich aus.

- Vermeiden Sie es, Einträge mit der Einstellung *Ablehnen* zu verwenden. Zugriffsverbote können sehr schnell zu unbeabsichtigten Nebenwirkungen führen. Im schlimmsten Fall verlieren alle Benutzer Zugriff auf ein Objekt und die Einstellung kann nicht mehr rückgängig gemacht werden. Ablehnungseinträge sollten speziellen Sonderfällen vorbehalten bleiben und der Systemverwalter sollte sich notieren, an welcher Stelle er einen Ablehnungseintrag aus welchem Grund angelegt hat.

- Wenn ein Problem mit einer Berechtigung auftritt, z.B. wenn einem Benutzer unerwartet der Zugriff auf ein Objekt verweigert wird, lassen Sie sich vom System nicht nur die reine ACL anzeigen, sondern lassen Sie Mac OS X die ACL abarbeiten, so dass das tatsächlich wirksame Zugriffsrecht berechnet wird.

Hierzu gibt es z.B. im Arbeitsgruppen-Manager die Ansicht TATSÄCHLICHE ZUGRIFFSRECHTE. Das Arbeiten mit ACLs wird im nachfolgenden Abschnitt noch genauer erläutert.

- Schützen Sie nicht nur Ihre Datendateien, sondern auch alle installierten Programme. Um den einwandfreien Betrieb zu garantieren, ist es sinnvoll, nur der Personengruppe, die Programme installieren darf, Schreibrecht auf die Programme zu geben. Dies bewahrt Sie vor absichtlicher oder unabsichtlicher Beschädigung der Programme, z.B. durch Bedienungsfehler, unzufriedene Mitarbeiter, unkooperative Schüler oder Studierende, trojanische Pferde und Computerviren. Der Schutz wird weiter erhöht, wenn getrennte Benutzerkonten für die Installation von Programmen und die normale Nutzung des Computers verwendet werden. Im Normalfall ist dann kein Benutzer am System angemeldet, der Programme ändern könnte.

5.4 Arbeiten mit ACLs

5.4.1 ACLs in der grafischen Oberfläche

Das Arbeiten mit ACLs auf der grafischen Oberfläche von Mac OS X steht nur in der Serverversion des Betriebssystems zur Verfügung, da hierzu das Programm *Arbeitsgruppen-Manager* verwendet werden muss. In der Standardversion müssen Sie entweder die Kommandozeile oder Programme von Drittanbietern einsetzen.

Wir erläutern das Anlegen eines ACEs an folgendem Beispiel:

1. Starten Sie den Arbeitsgruppen-Manager und verbinden Sie sich mit dem gewünschten Server.
2. Wählen Sie in der Symbolleiste den Punkt SHARING aus.
3. Wählen Sie in der linken Hälfte des Fensters entweder über NETZWERKORDNER oder ALLE einen Ordner oder eine Datei aus, für den Sie einen Zugriffssteuerungseintrag anlegen möchten.
4. Wählen Sie in der rechten Hälfte des Fensters den Punkt ZUGRIFF aus. Im oberen Teil der Anzeige erscheinen die POSIX-Berechtigungseinstellungen, die Sie bereits kennen. Der untere Teil enthält die Zugriffssteuerungsliste (Abbildung 5.2).
5. Drücken Sie den Knopf BENUTZER UND GRUPPEN, um ein Schubfach mit den zur Verfügung stehenden Benutzer- und Gruppenkonten zu öffnen. Es werden alle Benutzer und Gruppen mit GUIDs aus dem gewählten Verzeichnisknoten angezeigt.
6. Ziehen Sie einen Benutzer- oder Gruppeneintrag mit der Maus in die Zugriffssteuerungsliste. Ein neuer ACE wird eingerichtet.

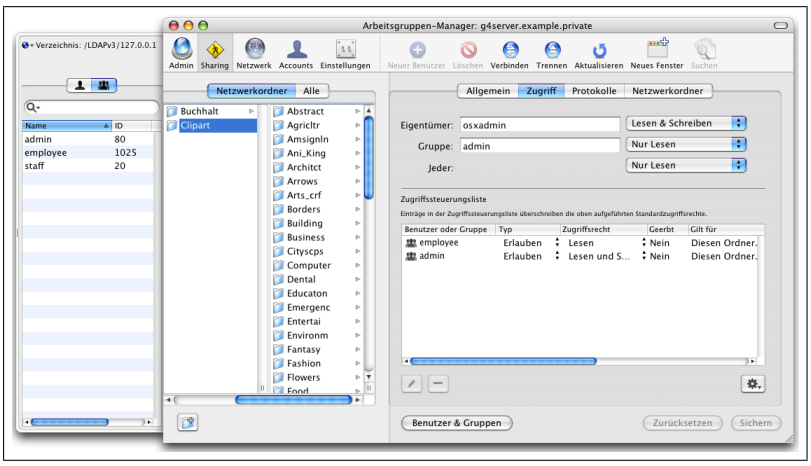

Abbildung 5.2: Der Arbeitsgruppen-Manager ermöglicht den bequemen Zugriff auf Zugriffssteuerungslisten über die grafische Oberfläche

7. Klicken Sie in der betreffenden Zeile auf den Eintrag in der Spalte TYP, um entweder die Einstellung *Erlauben* oder die Einstellung *Ablehnen* auszuwählen.

8. Klicken Sie nach gleicher Methode auf den Inhalt der Spalte ZUGRIFFSRECHT, um das gewünschte Zugriffsrecht für diesen ACE zu definieren. Apple hat vier Standardeinstellungen, nämlich VOLLSTÄNDIGE STEUERUNG (alle Rechte), LESEN UND SCHREIBEN, nur LESEN und nur SCHREIBEN bereits in einem Aufklappmenü vorgesehen. Wenn Sie frei zwischen allen 13 Möglichkeiten der Zugriffsdefinition und den 4 Möglichkeiten der Vererbung entscheiden möchten, klicken Sie auf den Punkt ANGEPASST. Es öffnen sich dann ein vergrößerbares Klappfenster, in dem alle 98.304 Kombinationen von Einstellungen durch Ankreuzen der Optionen gemacht werden können (Abbildung 5.3).

9. Drücken Sie auf SICHERN, um den neuen ACE abzuspeichern.

In der Spalte GEERBT der Tabelle können Sie außerdem ablesen, ob das gerade ausgewählte Dateisystemobjekt einen wirklich „eigenen" Eintrag besitzt, oder ob eine ACL von einem übergeordneten Ordner geerbt wurde. Die letzte Spalte GILT FÜR, die sehr breit werden kann, formuliert noch einmal im Klartext, welche Vererbungseinstellungen in diesem ACE wirksam sind.

Um einen bereits bestehenden Zugriffssteuerungseintrag zu ändern, wählen Sie den Eintrag in der Tabelle aus und drücken Sie den mit einem Stift markierten Knopf unterhalb der Tabelle. Um einen ACE zu löschen, betätigen Sie die Schaltfläche, die mit einem großen Minuszeichen markiert ist.

Falls Sie die obigen Schritte einmal mit einem gefüllten Ordner Ihres Servers ausprobieren, werden Sie bemerken, dass danach die im Ordner enthaltenen Objekte wie

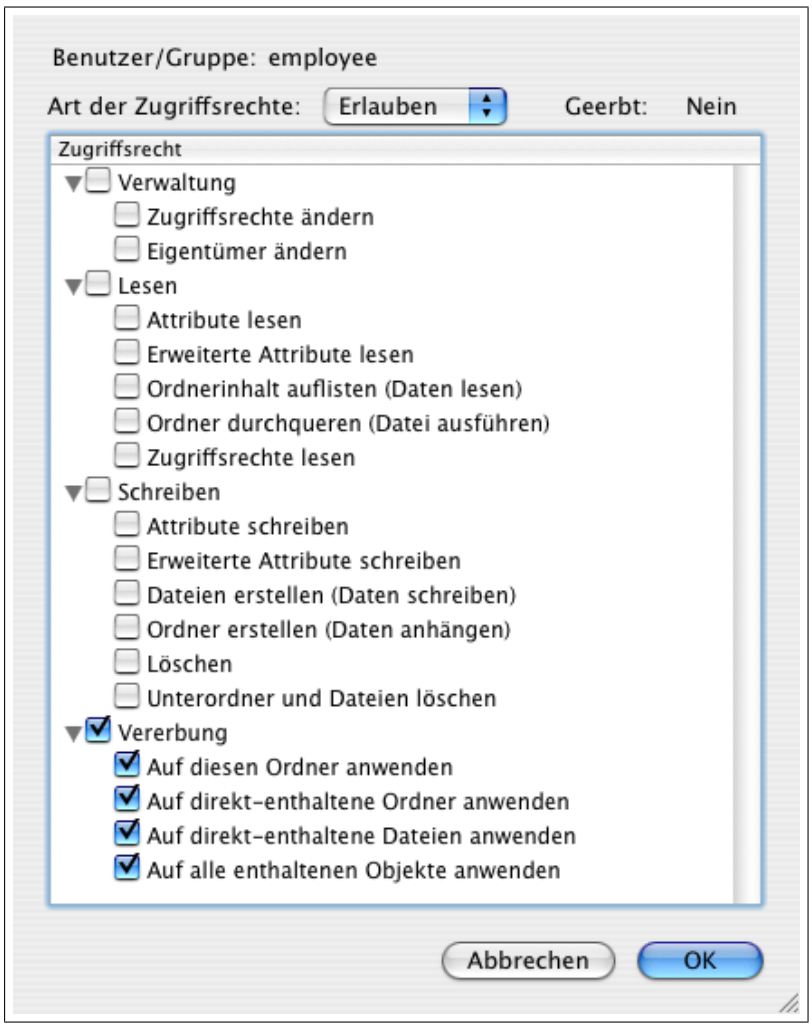

Abbildung 5.3: Über den Punkt ANGEPASST können alle Zugriffs- und Vererbungsdefinitionen im Detail eingestellt werden.

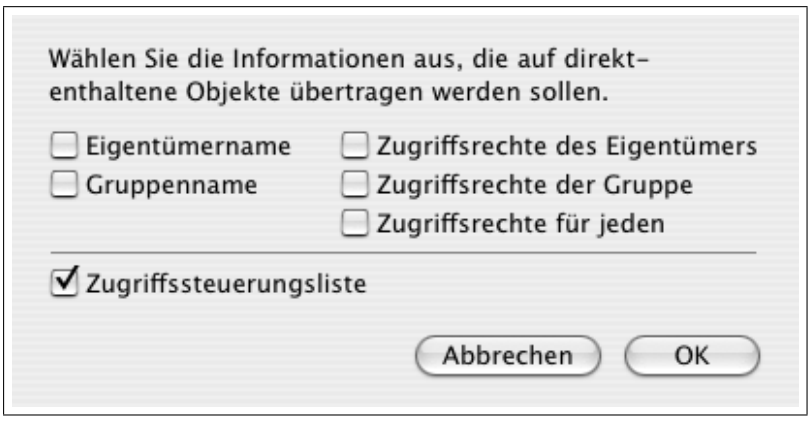

Abbildung 5.4: Über dieses Dialogfenster wird der Arbeitsgruppen-Manager veranlasst, POSIX- und ACL-Attribute an weiter unten in der Ordnerhierarchie liegende Objekte zu vererben, auch wenn keine neuen Objekte angelegt werden.

vorher *keine* Zugriffssteurungseinträge besitzen, auch wenn alle Vererbungsoptionen eingeschaltet waren. Dies ist das erwartete und richtige Verhalten. Erinnern Sie sich daran, dass die Vererbung nur dann aktiv wird, wenn Sie ein *neues* Objekt in der betreffenden Ordnerhierarchie anlegen, oder wenn Sie ein Programm ausdrücklich anweisen, die Vererbung nun auf die enthaltenen Unterobjekte anzuwenden. Um dies im Arbeitsgruppen-Manager durchzuführen, drücken Sie den mit einem Zahnrad markierten Knopf unterhalb der Tabelle und wählen Sie den Menüpunkt ZUGRIFFSRECHTE ÜBERTRAGEN... aus. Es erscheint das Dialogfenster aus Abbildung 5.4, mit dem Sie steuern können, welche Attribute Sie nun auf die untergeordneten Objekte kopieren möchten. Die obere Hälfte des Dialogfenster bezieht sich auf die POSIX-Einstellungen, die untere Hälfte, die nur aus der Option ZUGRIFFSSTEUERUNGSLISTE besteht, auf die ACL.

Einträge in der Zugriffssteuerungsliste, die „von oben" geerbt wurden, erscheinen in der Tabelle grau. Sie können einen solchen geerbten Eintrag nicht als solchen ändern, aber er lässt sich löschen. Sie können auch alle geerbten Einträge gleichzeitig löschen, indem Sie im Menü der Zahnrad-Schaltfläche den Punkt GEERBTE EINTRÄGE ENTFERNEN auswählen.

Um einen geerbten Eintrag in einem untergeordneten Teilbaum der Ordnerhierarchie doch ändern zu können, müssen Sie den Menüpunkt GEERBTE EINTRÄGE DURCH EXPLIZITE ERSETZEN verwenden. Auch in diesem Fall werden die von oben ererbten Zugriffssteuerungseinträge zunächst gelöscht, sie werden aber danach als „echte" Einträge für dieses Objekt neu angelegt. Dadurch haben Sie anschließend die Möglichkeit, die Detaileinstellungen des ACE wie gewünscht anzupassen.

Der Auswertungsmechanismus der übernommenen und expliziten Zugriffssteuerungseinträge macht es im Einzelfall schwer, nachzuvollziehen, welche Berechtigung für ein bestimmtes Objekt denn nun wirklich aktiv wird. Der Arbeitsgruppen-Manager stellt hierzu eine bequeme Hilfe bereit: Sie können sich für ein beliebi-

Abbildung 5.5: Welche Rechte tatsächlich auf einem Dateisystemobjekt wirksam werden, kann man sich für jeden Benutzeraccount in diesem Fenster berechnen lassen.

ges Dateisystemobjekt und für ein beliebiges Benutzerkonto die aktuelle Zugriffsberechtigung von Mac OS X ausrechnen lassen. Verwenden Sie hierzu den Punkt DETAILANSICHT FÜR TATSÄCHLICHE ZUGRIFFSRECHTE ANZEIGEN im Zahnrad-Menü nachdem Sie ein Objekt im Dateisystem ausgewählt haben. Es erscheint ein Fenster wie in Abbildung 5.5. Ziehen Sie nun einen Benutzereintrag aus dem Schubfach über das Feld BENUTZER, so wird die effektive Berechtigung ausgewertet und das Ergebnis durch Häkchen bei den entsprechenden Optionsfeldern angezeigt.

Falls Sie mit Zugriffssteuerungslisten auf einem Datenträger arbeiten möchten, der nachträglich hinzugefügt wurde, beispielsweise bei einer Wechselplatte oder einem extern angeschlossenen Plattenlaufwerk, so behandelt Mac OS X das Volume standardmäßig ohne Berücksichtigung von Benutzerrechten. Sie müssen in diesem Fall erst die Funktion ZUGRIFFSSTEUERUNGSLISTEN AUF DIESEM VOLUME AKTIVIEREN in der Rubrik ALLGEMEIN des Bereichs SHARING ankreuzen, bevor Sie mit ACLs arbeiten können.

5.4.2 Verschachtelte Gruppen im Arbeitsgruppen-Manager

Das Anlegen von verschachtelten Gruppen im Arbeitsgruppen-Manager funktioniert wie erwartet: Angenommen Sie haben eine übergeordnete Gruppe A, in die Sie eine Gruppe B integrieren möchten, dann ziehen Sie einfach im Arbeitsgruppen-Manager das Gruppenkonto von B in die Mitgliedertabelle von A.

Machen Sie sich bewusst, was passiert, wenn ein Benutzer nun Mitglied der Gruppe B ist: Da B selbst ein Mitglied der Gruppe A ist, wird dieser Benutzer *automatisch* auch Mitglied der übergeordneten Gruppe A. Im Arbeitsgruppen-Manager wird dies als *geerbte Gruppe* bezeichnet. Sie können das Erben von Gruppenmitgliedschaften auf Wunsch im Arbeitsgruppen-Manager anzeigen lassen. Das System berechnet auf Knopfdruck, wie die tatsächliche Gruppenmitgliedschaft eines Benutzers aussieht. Geerbte Gruppen werden hierbei durch kursive Schrift dargestellt (Abbildung 5.6):

1. Stellen Sie sicher, dass im Arbeitsgruppen-Manager das Symbol ACCOUNTS ausgewählt ist, und wählen Sie in der Account-Liste ein Benutzerkonto aus.

2. Gehen Sie im rechten Teil des Fensters zur Rubrik GRUPPEN.

3. Betätigen Sie die Schaltfläche GEERBTE GRUPPEN EINBLENDEN unter der Mitgliedschaftstabelle. Mac OS X notiert neben dem Knopf, auf welchem Stand die aktuelle Mitgliedschaftsberechnung basiert und blendet eventuell vorhandene geerbte Gruppen in kursiver Schrift in die Tabelle ein.

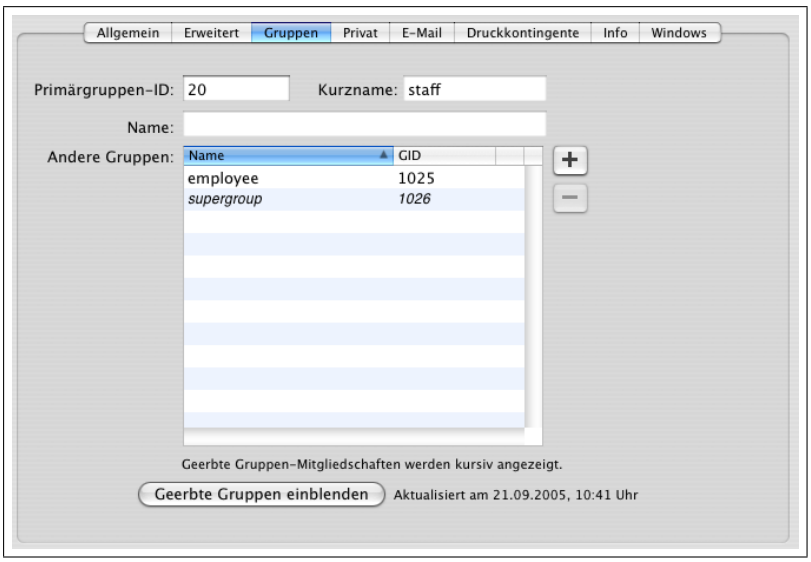

Abbildung 5.6: Durch die GUID-Technik der ACLs lassen sich auch verschachtelte Gruppen anlegen. Bezüglich der Benutzerkonten entstehen daraus geerbte Gruppenmitgliedschaften, die im Arbeitsgruppen-Manager per Knopfdruck dargestellt werden können.

5.4.3 Einstellung von SACLs

Um auch den Zugriff auf Dateiserverdienste über ACLs steuern zu können, müssen Sie das Programm *Server Admin* verwenden. Wir erläutern dies am Beispiels des AFP-Servers:

1. Starten Sie das Programm *Server Admin* und verbinden Sie sich mit dem betreffenden Server.

2. Wählen Sie in der Liste COMPUTER & DIENSTE den Servereintrag selbst aus, nicht einen seiner Untereinträge.

3. Klicken Sie in der rechten Hälfte des Bildes auf den Punkt EINSTELL..

4. Wählen Sie die Rubrik ZUGRIFF aus.

5. Entfernen Sie das Häkchen bei GLEICHER ZUGRIFF FÜR ALLE DIENSTE.

6. Wählen Sie in der linken Tabelle einen Dienst aus, für den Sie eine SACL einrichten möchten.

7. Schalten Sie die Auswahl über der rechten Tabelle auf den Knopf NUR BENUTZER UND GRUPPEN UNTEN: um.

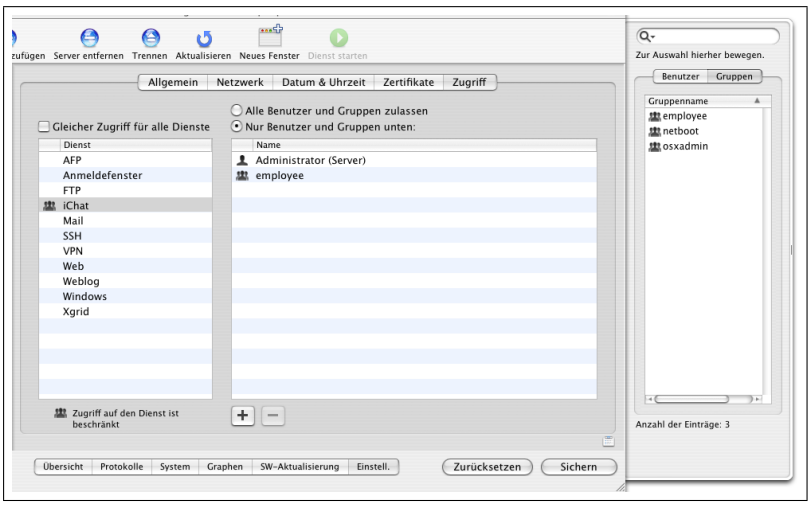

Abbildung 5.7: In Tiger können auch bestimmten Netzwerkdiensten Zugriffssteuerungslisten, sogenannte SACLs, zugewiesen werden.

8. Nutzen Sie die Plus-Schaltfläche unter der Tabelle, um über das erscheinende Schubfach Benutzer oder Gruppen in die Tabelle NAME zu ziehen. Hiermit wird das entsprechende Zugriffsrecht auf den Dienst erteilt. Ein Eintrag kann mit der Minus-Schaltfläche wieder entfernt werden.

5.4.4 ACLs auf der Kommandozeile

Die bekannten Befehle *ls* zum Anzeigen von Ordnerinhalten und *chmod* zum Ändern von Berechtigungseinstellungen wurden in Mac OS X Tiger so erweitert, dass sie jetzt auch mit ACLs umgehen können. Wenn Sie einen Ordner im Langformat (Option *-l*) auflisten lassen, so markiert Mac OS X das Vorhandensein einer ACL mit einem zusätzlichen Pluszeichen neben den POSIX-Markierungen:

```
g4server:/Public osxadmin$ ls -l
total 0
drwxr-xr-x    2 osxadmin  admin    68 Sep 20 12:27 Buchhaltung
drwxr-xr-x + 63 osxadmin  admin  2142 Jun 14  2002 Clipart
drwxr-xr-x    2 osxadmin  admin    68 Sep 20 12:28 Marketing
```

In diesem Beispiel ist der Unterordner *Clipart* mit einer ACL versehen. Um sich den Ordner inklusive der ACLs anzeigen zu lassen, fügen Sie dem ls-Befehl einfach die Option *-e* hinzu. Hier das entsprechende Beispiel:

```
g4server:/Public osxadmin$ ls -le
```

Einstellung	Schlüsselwort
Zugriff erlauben	`allow`
Zugriff ablehnen	`deny`
Daten lesen	bei Dateien: `read` bei Ordnern: `list`
Daten ausführen / durchqueren	bei Dateien: `execute` bei Ordnern: `search`
Attribute lesen	`readattr`
Erweiterte Attribute lesen	`readextattr`
Zugriffsrechte lesen	`readsecurity`
Daten schreiben	bei Dateien: `write` bei Ordnern: `add_file`
Daten anhängen	bei Dateien: `append` bei Ordnern: `add_subdirectory`
Attribute schreiben	`writeattr`
Erweiterte Attribute schreiben	`writeextattr`
Zugriffsrecht ändern	`writesecurity`
Eigentümer ändern	`chown`
Löschen	`delete`
Unterordner löschen	`delete_child`
auf diesen Ordner anwenden	`limit_inherit`
auf unmittelbare Unterordner vererben	`directory_inherit`
auf unmittelbar enthaltene Dateien vererben	`file_inherit`
auf weiter unten enthaltene Objekte vererben	`only_inherit`

Tabelle 5.2: Schlüsselworte, mit denen ACLs auf der Kommandozeile notiert werden

```
total 0
drwxr-xr-x    2 osxadmin  admin    68 Sep 20 12:27 Buchhaltung
drwxr-xr-x + 63 osxadmin  admin  2142 Jun 14  2002 Clipart
 0: group:employee allow list,search,readattr,readextattr,
 readsecurity,file_inherit,directory_inherit
 1: group:admin allow list,add_file,search,delete,add_subdirectory,
 delete_child,readattr,writeattr,readextattr,writeextattr,
 readsecurity,file_inherit,directory_inherit
drwxr-xr-x    2 osxadmin  admin    68 Sep 20 12:28 Marketing
```

Referenzen auf GUIDs werden in Klartext nach dem Muster `user:benutzername` aufgelöst, wenn es sich um ein Benutzerkonto handelt, bzw. `group:gruppenname`, falls es sich um ein Gruppenkonto handelt. Für die Übersetzung der Begriffe *Erlauben, Ablehnen* sowie den Zugriffs- und Vererbungseinstellungen in Schlüsselworte für die Kommandozeile verwenden Sie bitte Tabelle 5.2.

Um nun die ACLs von Dateisystemobjekten manipulieren zu können, wurden dem chmod-Befehl neue Optionen hinzugefügt:

- `+a` *schlüsselworte* bewirkt, dass einem Dateisystemobjekt ein über die Schlüsselworte angegebener ACE hinzugefügt wird
- `+ai` *schlüsselworte* fügt einen ACE ebenso hinzu, erzwingt jedoch, dass der Eintrag als vererbt markiert wird
- `+a#` *n schlüsselworte* fügt einen ACE an die n-te Position in der ACL ein
- `+ai#` *n schlüsselworte* fügt einen ACE an die n-te Position in der ACL ein und erzwingt, dass der Eintrag als vererbt markiert wird
- `-a` *schlüsselworte* löscht den gegebenen ACE
- `-a#` *n* löscht den ACE an der n-ten Position der ACL
- `=a#` *n schlüsselworte* ersetzt den ACE an der n-ten Position der ACL durch den angegebenen Eintrag
- `-i` entfernt alle Markierungen, dass ACEs geerbt sind, aus der gesamten ACL
- `-I` entfernt alle ACEs, die als geerbt markiert sind

Benutzer- und Gruppenangaben sollten bei Verwendung des Befehls *chmod* über deren Kurznamen erfolgen. Die Schlüsselworte `group` und `user` dürfen nicht verwendet werden. Das Kommando versucht, die Kurznamen auch ohne diese Angaben automatisch dem richtigen Kontotyp zuzuweisen. Liegen gleichnamige Gruppen- und Benutzerkonten im System vor, hat der Benutzereintrag Vorrang. Die oben erwähnten Schlüsselworte werden durch Kommas voneinander getrennt. Hier ein paar Beispiele und ihre Wirkung:

```
g4server:~ osxadmin$ mkdir acltest
g4server:~ osxadmin$ cd acltest
g4server:~/acltest osxadmin$ touch datei1 datei2
g4server:~/acltest osxadmin$ ls -l
total 0
-rw-r--r--   1 osxadmin  osxadmin  0 Sep 20 19:26 datei1
-rw-r--r--   1 osxadmin  osxadmin  0 Sep 20 19:26 datei2
g4server:~/acltest osxadmin$ chmod +a "admin allow write,delete" datei1
g4server:~/acltest osxadmin$ ls -le
total 0
-rw-r--r-- + 1 osxadmin  osxadmin  0 Sep 20 19:26 datei1
 0: group:admin allow write,delete
-rw-r--r--   1 osxadmin  osxadmin  0 Sep 20 19:26 datei2
g4server:~/acltest osxadmin$ chmod +a "employee deny delete" datei1
g4server:~/acltest osxadmin$ ls -le
total 0
-rw-r--r-- + 1 osxadmin  osxadmin  0 Sep 20 19:26 datei1
 0: group:employee deny delete
 1: group:admin allow write,delete
-rw-r--r--   1 osxadmin  osxadmin  0 Sep 20 19:26 datei2
```

```
g4server:~/acltest osxadmin$ chmod +ai "employee allow append" datei1
g4server:~/acltest osxadmin$ ls -le
total 0
-rw-r--r-- + 1 osxadmin  osxadmin  0 Sep 20 19:26 datei1
 0: group:employee deny delete
 1: group:admin allow write,delete
 2: group:employee inherited allow append
-rw-r--r--   1 osxadmin  osxadmin  0 Sep 20 19:26 datei2
g4server:~/acltest osxadmin$ chmod -a# 2 datei1
g4server:~/acltest osxadmin$ ls -le
total 0
-rw-r--r-- + 1 osxadmin  osxadmin  0 Sep 20 19:26 datei1
 0: group:employee deny delete
 1: group:admin allow write,delete
-rw-r--r--   1 osxadmin  osxadmin  0 Sep 20 19:26 datei2
```

Um die Unterstützung von ACLs auf einem Volume einzuschalten, bei dem dies noch nicht automatisch geschehen ist, verwenden Sie das neue Kommando *fsaclctl (file system access control list control)*. Der Befehl

```
fsaclctl -p einblendungspunkt
```

zeigt an, ob auf einem bestimmten Volume die Unterstützung von ACLs ein- oder ausgeschaltet ist. Hierbei muss an der Position *einblendungspunkt* eine Unix-Pfadangabe für den Einblendungspunkt *(Mount Point)* des entsprechenden Volumes gesetzt werden, zum Beispiel:

```
g4server:~ osxadmin$ fsaclctl -p /
Access control lists are supported on /.
```

Fügen Sie zusätzlich die Option `-e` hinzu, so wird die Unterstützung von ACLs auf diesem Volume eingeschaltet. Fügen Sie dagegen die Option `-d` hinzu, so wird die Unterstützung für dieses Volume abgeschaltet. Hierbei werden alle ACLs auf dem Volume entfernt und unwirksam, es gelten danach nur noch die klassischen POSIX-Attribute.

Wenn Sie auf einem Tiger-Server professionelle Datensicherung auf Band durchführen, müssen Sie mit dem Einsatz von ACLs sehr vorsichtig sein: In den meisten aktuellen Datensicherungsprogrammen ist die Verwendung von ACLs noch nicht berücksichtigt. Wenn Sie eine Datensicherung mit einem solchen Programm durchführen, werden zwar die Dateiinhalte, die Forks und alle POSIX-Attribute gesichert, nicht jedoch die Zugriffssteuerungslisten. Nur die zu Mac OS X selbst gehörenden Sicherungsprogramme wie *ditto* und *asr*, sowie alle Drittanbieterprogramme zum „Klonen“ von Systeminstallationen, die auf diesen beiden Mac OS X-Programmen beruhen, beherrschen im Moment ACLs.

Für das im Hauptbuch erwähnte Datensicherungsprogramm *Retrospect* hat der Hersteller EMC Dantz für Ende 2005 die Unterstützung der ACLs von Tiger angekündigt. Voraussichtlich wird im Laufe des Oktobers die Version 6.1 lieferbar sein, die ACLs unterstützen soll. Prüfen Sie bei der Verwendung anderer Sicherungsprogramme, ob oder wann der jeweilige Hersteller ACLs unterstützen wird.

Kapitel 6

Benutzer, Gruppen und Computer

6.1 Ortsungebundene Benutzer

6.1.1 Neue Funktionen

Apple hat das Funktionsmerkmal zur Unterstützung ortsungebundener Konten weiter ausgebaut. Die Hauptneuerung ist, dass nicht nur die reinen Kontodaten eines Benutzers zwischen einem mobilen Computer und einem Server automatisch abgeglichen werden, es lässt sich nun auch steuern, dass die *Dateien* dieses Benutzers zwischen der Festplatte des Mobilcomputers und einem zentralen Netzwerkordner synchronisiert werden.

Dies ermöglicht es dem Benutzer eines Notebooks, „wenn er gerade im Hause ist" seinen privaten Ordner zentral auf dem Fileserver zu halten, aber „wenn er gerade unterwegs ist" und keine Verbindung zum Netz hat, mit einer Kopie seiner aktuellen Daten auf der Festplatte des Notebooks zu arbeiten. Kehrt der Benutzer später wieder zurück, werden die unterwegs gemachten Änderungen wieder mit seinem Privatordner auf dem Fileserver abgeglichen.

Die Steuerung dieser neuen Funktion ist über zusätzliche verwaltete Einstellungen möglich, die an ein Benutzerkonto (oder andere Konten) geknüpft werden können. Der betreffende Benutzer wird damit zum *mobilen Benutzer*. Die Einstellungen werden über den Arbeitsgruppen-Manager vorgenommen (Abbildung 6.1):

1. Starten Sie den Arbeitsgruppen-Manager und verbinden Sie sich mit dem Verzeichnisdienstserver, der das betreffende Benutzerkonto enthält.
2. Wählen Sie in der linken Spalte die Benutzer-Rubrik aus und klicken Sie das betreffende Benutzerkonto an.
3. Klicken Sie in der Symbolleiste des Programms auf EINSTELLUNGEN.

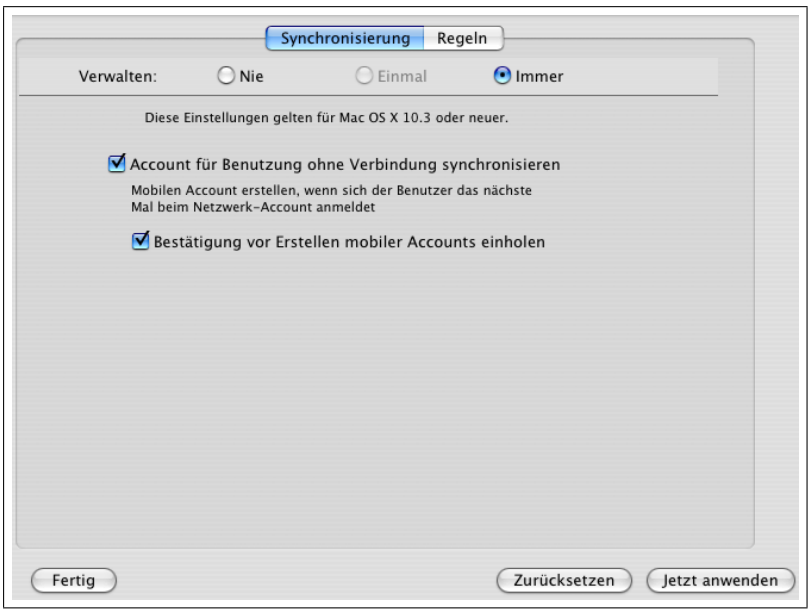

Abbildung 6.1: Über die verwalteten Einstellungen kann ein Benutzer zum mobilen Nutzer gemacht werden.

4. Wählen Sie in der rechten Hälfte die Rubrik MOBILITÄT.
5. Schalten Sie auf der Karteikarte SYNCHRONISIERUNG die Option VERWALTEN auf den Punkt IMMER.
6. Kreuzen Sie den Punkt ACCOUNT FÜR BENUTZUNG OHNE VERBINDUNG SYNCHRONISIEREN an.

Der ausgewählte Benutzer wird damit zu einem mobilen Benutzer. Falls Sie dem Benutzer die Wahl lassen möchten, ob er beim nächsten Anmeldevorgang wirklich zum mobilen Benutzer werden soll, kreuzen Sie zusätzlich den Punkt BESTÄTIGUNG VOR ERSTELLEN MOBILER ACCOUNTS EINHOLEN an. Meldet sich der Benutzer nun an seinem Mobilcomputer an, so wird er erst gefragt, ob er seine Kontodaten wirklich mit dem Verzeichnisdienst synchronisieren will. Er kann damit immer noch ablehnen, zum mobilen Benutzer zu werden (Abbildung 6.2).

Ist die Mobilitätsfunktion aktiv geworden, werden nun in jedem Fall die Account-Daten dieses Benutzers, zum Beispiel Kennwortänderungen, zwischen dem lokalen Verzeichnisdienst des „eigenen" Computers dieses Benutzers und dem zentralen Verzeichnisdienstserver synchronisiert. Zusätzlich steht ab Mac OS X 10.4 die neue Funktion zur Verfügung private Dateien zwischen der Festplatte des „eigenen" Computers und einem zentralen Dateiserver automatisch abgleichen zu lassen. Beachten Sie hierbei die folgenden wichtigen Hinweise:

- Die Nutzung dieser Funktion setzt voraus, dass der mobile Benutzer an einen

Möchten Sie jetzt einen portablen Ordner „Privat“ auf diesem Computer erstellen?
Ein portabler Ordner „Privat“ enthält eine synchronisierte Kopie Ihres Netzwerk-Accounts, falls dieser Computer vom Netzwerk getrennt wird.
Später
Nie
Ja

Abbildung 6.2: Je nach Einstellung darf der Benutzer bei seiner nächsten Anmeldung ablehnen, dass er zum mobilen Nutzer wird.

bestimmten mobilen Computer geknüpft ist. Der Benutzer kann zwar im lokalen Netz zwischen beliebigen, ständig mit dem Netz verbundenen Computern hin- und her wechseln (freies Roaming), er darf aber nicht zwischen mehreren mobilen, also nicht mit dem Netz verbundenen Computern wechseln, da es ansonsten zu Problemen kommen kann, die Daten korrekt nachzuverfolgen.

- Sie müssen die Mobilitätsfunktion nicht unbedingt an ein Benutzerkonto knüpfen. Sie können ebenso ein Gruppenkonto oder ein Computerlistenkonto verwenden. Hierbei werden dann alle Benutzer der Gruppe, bzw. alle Benutzer der entsprechenden Computer als mobil markiert.
- Die Synchronisation von Dateien ist nur möglich, wenn sowohl auf dem Server als auch auf dem mobilen Client mindestens Mac OS X 10.4 verwendet wird.
- Die Detaileinstellungen, welche Dateien zu welchen Zeitpunkten automatisch abgeglichen werden, werden mit dem Punkt REGELN bei den verwalteten Mobilitätseinstellungen im Arbeitsgruppen-Manager vorgenommen. Dies wird im nachfolgenden Abschnitt erläutert.
- Verbindet sich ein mobiler Nutzer zum ersten Mal mit dem Netz, so kann dessen mobiler Privatordner auf den Fileserver kopiert werden. Automatisch ist dies beim ersten Mal nur dann möglich, wenn AFP als Protokoll für den Privatordnerzugriff konfiguriert ist, bei anderen Protokollen (NFS oder CIFS/SMB) muss die erste Synchronisation manuell erfolgen.
- Ebenso darf die allererste Verbindung zum Netz nicht über ein VPN erfolgen, selbst wenn für den Dateizugriff AFP verwendet wird. Erst nachdem die erste Synchronisation des Privatordners erfolgt ist, kann ein VPN eingesetzt werden.
- Bedenken Sie die Konsequenzen für Ihre Datenschutz- und Datensicherheitsrichtlinien, wenn sie ortsungebundene, synchronisierte Privatordner einset-

zen. Dateien, die auf der lokalen Offline-Kopie geändert oder neu angelegt werden, nehmen so lange nicht an einer zentralen Datensicherung des Fileservers teil, bis die nächste Synchronisierung stattgefunden hat. Da die mobilen Privatordner Kopien von Daten des Fileservers enthalten, die sich vom Netz weg in möglicherweise nicht vertrauensvolle Umgebungen bewegen, überlegen Sie, ob Sie nicht zusätzliche Schutzmaßnahmen – wie die Verschlüsselung über FileVault, das Einrichten von Open Firmware-Kennworten auf allen Mobilcomputern, etc. – etablieren müssen.

6.1.2 Einrichten der Synchronisationsregeln für private Dateien

Nicht verwaltete Einstellungen

Sind keine verwalteten Einstellungen für die Synchronisation privater Dateien definiert, aber ein ortsungebundener Benutzer verwendet Mac OS X Tiger auf einem Clientcomputer, so verwendet dieser Computer Standardwerte für die Synchronisation. Der Benutzer sieht an einem zusätzlichen Menüleistensymbol (Abbildung 6.3), dass für seinen Privatordner Synchronisationsfunktionen zur Verfügung stehen. Er kann diese auch manuell über das daran hängende Menü aufrufen und sie im Detail selbst konfigurieren.

Die Konfiguration findet statt, indem der Benutzer den Punkt EINSTELLUNGEN ZUR SYNCHRONISIERUNG VON „PRIVAT“... im Menüleistensymbol aufruft oder indem er das Programm *Systemeinstellungen* verwendet:

1. Starten Sie als ortsungebundener Benutzer das Programm *Systemeinstellungen*.

2. Wählen Sie die Rubrik BENUTZER aus.

3. Drücken Sie auf der Karteikarte den Knopf KONFIGURIEREN... neben dem Punkt MOBILEN ACCOUNT ERSTELLEN.

Es erscheint das Dialogfenster aus Abbildung 6.4. Mit dem Klappmenü SYNCHRONISIEREN können Sie einstellen, ob Mac OS X sich grundsätzlich automatisch um die Synchronisation kümmern soll, oder ob Sie als mobiler Benutzer die Synchronisation immer manuell auslösen möchten. Mit dem Knopf JETZT SYNCHRONISIEREN wird der Abgleich der Datenbestände sofort vorgenommen. In der Dateiübersicht in der Mitte des Fensters können Sie ein- und ausschalten, welche Unterordner Ihres privaten Ordners abgegelichen werden sollen. Hierzu können Sie die Knöpfe zwischen dem Punkt ALLE und AUSGEWÄHLTE ORDNER umschalten und die entsprechenden Ordner ankreuzen. Das Häkchen STATUS IN DER MENÜLEISTE ZEIGEN steuert, ob das Menüleistensymbol verwendet werden soll.

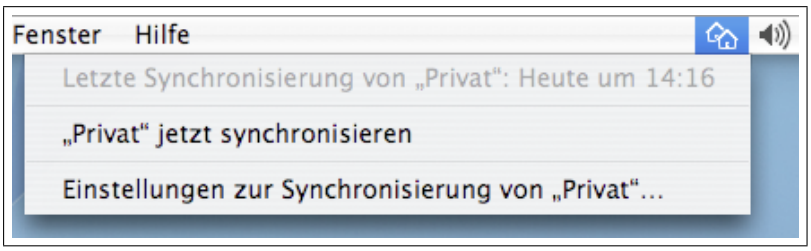
Fenster Hilfe
Letzte Synchronisierung von „Privat“: Heute um 14:16
„Privat“ jetzt synchronisieren
Einstellungen zur Synchronisierung von „Privat“…

Abbildung 6.3: Menüleistensymbol für mobile Dateisynchronisation

Beachten Sie, dass die Synchronisation der Daten sehr viel Zeit in Anspruch nehmen kann, wenn Sie mit großen Datenmengen, beispielsweise in der Videoproduktion, arbeiten oder Sie nur eine langsame Netzverbindung wie z.B. ein Airport-Funknetz zum Fileserver haben, der Ihren privaten Netzordner beherbergt.
Ist die Synchronisationszeit unakzeptabel lang, sollten Sie überlegen, die „großen“ Dateien in einen besonderen Ordner zu packen, der von der Synchronisation ausgeschlossen wird.

Verwaltete Einstellungen

Sollen die Einstellungen für die Synchronisation privater Dateien jedoch zentral verwaltet werden, müssen Sie den Arbeitsgruppen-Manager auf dem Server verwenden und auf die Karteikarte REGELN in der Einstellungsrubrik MOBILITÄT des entsprechenden Accounts wechseln. Hier stehen weitergehende Möglichkeiten zur Verfügung. Das Programm ist in der Lage, den Mobilcomputer anzuweisen, die automatische Synchronisation der Dateien entweder beim An- und Abmelden des ortsungebundenen Benutzers vorzunehmen, oder im Hintergrund, d.h. in wählbaren Zeitabständen während der Benutzer gerade angemeldet ist. Nach Ordnern gestaffelt können auch beide Verfahren gleichzeitig verwendet werden.

Im Punkt AN- UND ABMELDESYNCHRONISIERUNG wählen Sie die Objekte aus, die vor und nach der Benutzersitzung abgegelichen werden sollen, im Punkt HINTERGRUNDSYNCHRONISIERUNG die Objekte, die in regelmäßigen Abständen während der Benutzersitzung synchronisiert werden sollen. In beiden Fällen sind die Einstellmöglichkeiten gleich (Abbildung 6.5).

Die obere Tabelle erlaubt es, die Unterordner des privaten Ordners auswählen, die automatisch abgeglichen werden sollen. Das Drücken der Schaltfläche mit dem Pluszeichen legt einen neuen Eintrag an, der von Hand eingegeben werden muss. Beachten Sie, dass nur Objekte des Privatordners synchronisiert werden können, die Pfade müssen als BSD-Pfade relativ zum Privatordner angegeben werden, dürfen also nicht mit einem Schrägstrich beginnen. Denken Sie auch daran, dass die tatsächlichen Ordnernamen auf Systemebene nicht mit der übersetzten Darstellung der Namen im Finder übereinstimmen müssen. Apple bevorzugt für die relativen

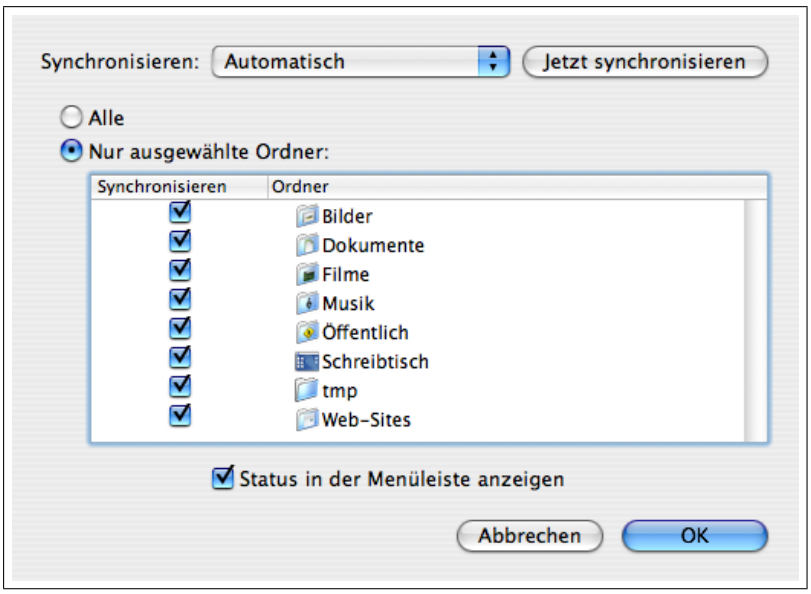

Abbildung 6.4: Anzeige der nicht verwalteten Synchronisationseinstellungen für einen ortsungebundenen Benutzer auf einem mobilen Computer

Pfade die übliche Unix-Schreibweise, bei der die Tilde als Platzhalter für den Privatordner verwendet wird.

Mit dem Minuszeichen lässt sich ein Eintrag wieder löschen, die drei Punkte erlauben die Auswahl von Ordnern über einen ÖFFNEN-Dateidialog. Hierbei ist allerdings zu beachten, dass zur Auswahl der Dateien der Privatordner des gerade mit dem Arbeitsgruppen-Manager arbeitenden Benutzers verwendet wird.

In der unteren Tabelle kann auf ähnliche Weise eine Ausschlussliste definiert werden. Hierbei stehen leistungsfähige Auswahlkriterien zur Verfügung. Sie können den eingegebenen Ausschlusstext mit einer der Bedingungen

- beginnt mit
- endet mit
- Name enthält
- Name ist
- Vollständiger Pfad
- Teilpfad

versehen und somit zur späteren Laufzeit komplexe Abfragen der relativen Dateipfade des jeweiligen Benutzers realisieren.

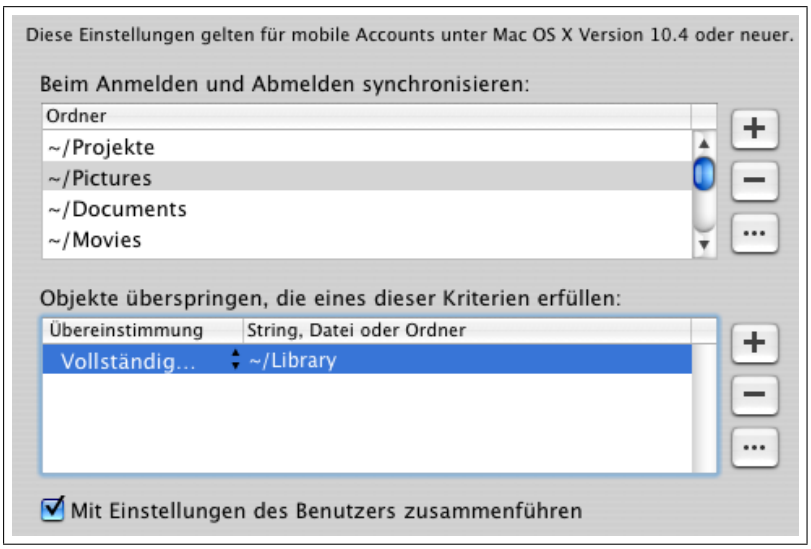

Abbildung 6.5: Über die verwalteten Einstellungen kann die gewünschte Betriebsart der Synchronisation auf dem Verzeichnisdienstserver noch exakter definiert werden.

Der Auswahlpunkt MIT EINSTELLUNGEN DES BENUTZERS ZUSAMMENFÜHREN bestimmt, ob die hier gemachten verwalteten Einstellungen mit den möglicherweise vorhandenen unverwalteten Einstellungen des jeweiligen Benutzers (siehe voriger Abschnitt) gemischt werden sollen. Bezüglich der Synchronisation im Hintergrund können Sie über die dritte Karteikarte OPTIONEN wählen, in welchen Zeitabständen die Synchronisation während einer Benutzersitzung stattfinden soll. Neben dem rein manuellen Betrieb kann ein Zeitintervall zwischen 5 und 60 Minuten ausgewählt werden.

6.2 Behandlung von Kennworten in Mac OS X Tiger

6.2.1 Zusätzliches Verfahren zur Prüfung von Kennworten

Neben den in Abschnitt 5.3.4 des Hauptbuchs genannten Verfahren zur Verschlüsselung und Überprüfung von Kennworten steht ab Version 10.4 des Betriebssystems das neue Verfahren *NTLMv2 (Windows Secure Password Exchange New Technology and LAN Manager Version 2)* zur Verfügung, das von neueren Windows-Versionen verwendet wird. Damit wird insbesondere die Kompatibilität mit Windows 2003 Server weiter erhöht. Falls Sie vorhaben, Benutzerkonten zu definieren, in denen die Kennworte der Benutzer ausschließlich über NTLMv2 überprüft werden, müssen Sie allerdings bedenken, dass ältere Versionen von Mac OS X damit nicht zurecht kommen.

6.2.2 Ausschließen bestimmter Verfahren zum Prüfen von Kennworten

Eine weitere neue Funktion in diesem Zusammenhang besteht darin, dass Sie nun gezielt die Nutzung bestimmter Verfahren zur Speicherung und Prüfung von Kennworten im Open Directory-Verzeichnisdienst verbieten können. Wie in Abschnitt 5.3.4 des Hauptbuchs erläutert, ist Open Directory in der Lage, Kennwort-Hashes auch für „fremde" Netzwerkdienste in jedem Benutzerkonto abzulegen. Je nach dem Verschlüsselungsverfahren, das für die Speicherung der Hashes zum Einsatz kommt, sind die unterschiedlichen Verfahren unterschiedlich sicher. Indem Sie alle in Ihrer Netzumgebung nicht gebrauchten Speicherungsverfahren ausschließen, können Sie die Sicherheit erhöhen, da ein Angreifer damit weniger Möglichkeiten hat, einen verschlüsselten oder gar unverschlüsselten Hash-Code zu analysieren. Dies wäre im Fall einer Offline-Attacke denkbar, bei dem es einem Angreifer bereits gelungen sein sollte, die physischen und logischen Schutzmaßnahmen eines Open Directory Servers- oder LDAP-Replikatsservers zu knacken und die Datei der Kennwortdatenbank auszulesen.

Apple bezeichnet in der deutschsprachigen Oberfläche von Mac OS X Tiger Kennwortprüfungsverfahren, die Kennworte unverschlüsselt ablegen, als *rückführbare Identifizierungsmethoden*. Gemeint ist damit, dass die abgelegten Kennworte entweder gar nicht oder nur so schwach verschlüsselt („verschleiert") sind, dass ein Angreifer, der es geschafft hat, einen Datenbankeintrag zu stehlen, aus den gespeicherten Daten das Kennwort wieder rückermitteln kann, ohne alle Möglichkeiten durchprobieren zu müssen.

Wenn Sie einzelne Identifizierungsmethoden deaktivieren, sollten Sie genau wissen, welche Methoden von den einzelnen Diensten und Softwareprodukten in Ihrem Netzwerk eingesetzt werden. In ungünstigen Fällen kann es passieren, dass sich durch das Abschalten eines Speicherverfahrens der gegenteilige Effekt ergibt: Schalten Sie zum Beispiel das Identifizierungsverfahren X auf dem Open Directory-Server ab, ein Dienst im Netzwerk verwendet jedoch das Verfahren X, um einen Benutzer beim Server zu identifizieren, so wird dieser Dienst sofort merken, dass die Methode X nun fehlschlägt. Einige Dienste sind jedoch so programmiert, dass sie in diesem Fall nicht aufgeben, sondern auf ein anderes, möglicherweise nicht verschlüsseltes Verfahren zur Benutzeridentifizierung umschalten. Zwar haben Sie in diesem Fall die Sicherheit der Kennwortdatenbank auf dem Server erhöht, im Netz aber vielleicht vermindert, da jetzt Dienste anfangen, Kennworte im Klartext über das Netz zu schicken, was sie mit dem vorigen Verfahren vielleicht nicht gemacht hätten. Aufgrund der Vielzahl der Betriebssysteme, Softwareprodukte und ihrer Netzwerkdienste lässt sich hier keine klare Empfehlung geben.

Das Sperren bestimmter Identifizierungsmethoden geschieht an unterschiedlichen Stellen, je nachdem, ob es sich um ein Benutzerkonto mit Shadow-Kennwort oder Kennworte in der Open Directory-Datenbank selbst handelt (siehe Abschnitt 5.3.3 des Hauptbuchs). Bei Shadow-Kennworten kann die Sperrung für jedes Benutzer-

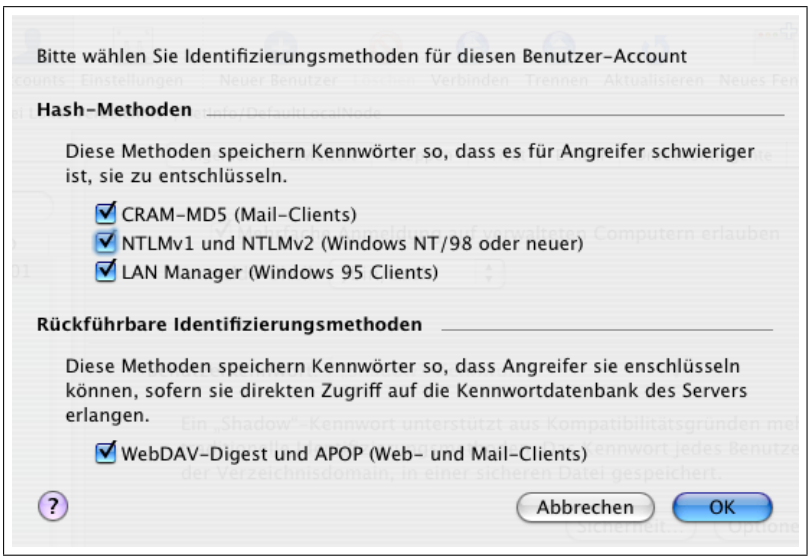
Bitte wählen Sie Identifizierungsmethoden für diesen Benutzer-Account
Hash-Methoden
Diese Methoden speichern Kennwörter so, dass es für Angreifer schwieriger ist, sie zu entschlüsseln.
CRAM-MD5 (Mail-Clients)
NTLMv1 und NTLMv2 (Windows NT/98 oder neuer)
LAN Manager (Windows 95 Clients)
Rückführbare Identifizierungsmethoden
Diese Methoden speichern Kennwörter so, dass Angreifer sie enschlüsseln können, sofern sie direkten Zugriff auf die Kennwortdatenbank des Servers erlangen.
WebDAV-Digest und APOP (Web- und Mail-Clients)
Abbrechen
OK

Abbildung 6.6: Bei Benutzerkonten mit Shadow-Kennworten können die zulässigen Identifizierungsmethoden ein- und ausgeschaltet werden.

konto einzeln im Arbeitsgruppen-Manager eingestellt werden, im Open Directory-Fall wird die Einstellung global für den ganzen Verzeichnisdienstserver geändert, wobei das Server-Admin-Programm zum Einsatz kommt.

Für den Fall eines Benutzerkontos mit Shadow-Kennwort:

1. Starten Sie den Arbeitsgruppen-Manager und verbinden Sie sich mit dem Server, der das betreffende Benutzerkonto enthält.
2. Wählen Sie in der Symbolleiste den Punkt ACCOUNTS aus.
3. Wählen Sie in der linken Hälfte des Fensters die Benutzerübersicht aus und wählen Sie den gewünschten Benutzer.
4. Öffnen Sie auf der rechten Seite des Fensters die Karteikarte ERWEITERT.
5. Klicken Sie im Abschnitt BENUTZERKENNWORT auf die Schaltfläche SICHERHEIT.... Dieser Knopf ist nur vorhanden, wenn es sich wirklich um einen Account mit Shadow-Kennwort handelt.
6. Im nun erscheinenden Dialogfenster (Abbildung 6.6) können einzelne Identifizierungsmethoden abgeschaltet werden. Das geänderte Konto ist mit Druck auf den Knopf SICHERN abzuspeichern.

Für den Fall der Speicherung der Kennworte in der Open Directory-Datenbank:

1. Starten Sie Server Admin und verbinden Sie sich mit dem betreffenden Server, der den Open Directory-Dienst beherbergt.

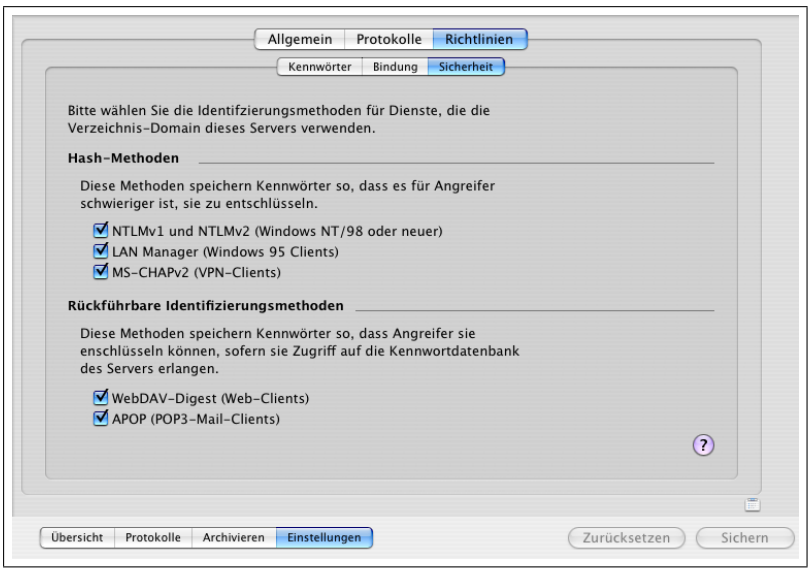

Abbildung 6.7: Sind die Kennworte in der Datenbank von Open Directory abgelegt, so können die zulässigen Speicher- und Überprüfungsmethoden in diesem dreifach verschachtelten Dialogfenster definiert werden.

2. Wählen Sie in der Tabelle COMPUTER & DIENSTE den Punkt OPEN DIRECTORY dieses Servers aus.

3. Wählen Sie auf der rechten Seite den Punkt EINSTELLUNGEN, dort die Karteikarte RICHTLINIEN und dort deren Unterpunkt SICHERHEIT.

4. Entfernen Sie die Häkchen der Identifizierungsmethoden, die Sie abschalten möchten (Abbildung 6.7).

5. Betätigen Sie die Schaltfläche SICHERN.

Es ist wichtig festzuhalten, dass durch das Sperren einzelner Identifizierungsmethoden die zugehörigen Kennworteinträge nicht sofort aus der Datenbank entfernt werden! Das ist technisch gar nicht möglich, denn um einen geänderten Eintrag in der Datenbank zu erstellen, ist Mac OS X gezwungen, Kennwort-Hashes neu abzuspeichern. Hierzu wird aber das Kennwort des Benutzerkontos benötigt, das Mac OS X im allgemeinen Fall nicht rückermitteln kann. Aus diesem Grund wird die Änderung in einem Benutzerkonto erst dann aktiv, wenn der Benutzer das nächste Mal sein Kennwort ändert. Der Netzverwalter kann natürlich die betreffenden Benutzerkonten mit den Möglichkeiten des Arbeitsgruppen-Managers zurücksetzen, so dass die Benutzer gezwungen werden, beim nächsten Anmeldevorgang ein neues Kennwort zu vergeben (was je nach Sicherheitsrichtlinien natürlich mit dem „alten“ identisch sein darf).

6.3 Der neue Kennwortassistent

Mac OS X Tiger enthält eine neue Funktion, mit der Sie beim Ändern Ihres Kennworts die Sicherheit des Kennworts neutral überprüfen lassen können. Ebenso können Sie sich ein neues Kennwort nach auswählbaren Sicherheitskriterien vom System erzeugen lassen. Diese neuen Funktionen werden über den *Kennwortassistenten* angeboten. Er steht immer dann zur Verfügung, wenn neben einem Feld zur Kennwortvergabe ein kleines Schlüsselsymbol angezeigt wird (Abbildung 6.8). Es erscheint ein Dialogfenster zur Vergabe oder Beurteilung von Kennworten.

Mit dem Klappmenü ART stellen Sie ein, wie Sie ein neues Kennwort anlegen möchten:

- **Manuell:** Sie geben das neue Kennwort selbst ein und der Assistent beurteilt, wie sicher das Kennwort ist. Ein Wort, das zu kurz ist oder in einem Wörterbuch nachgeschlagen werden kann, ist zum Beispiel sehr unsicher, da automatisierte Kennwortknackprogramme solche Worte in wenigen Minuten erraten können.
- **Einprägsam:** Bei Auswahl dieser Betriebsart werden Ihnen mehrere Kennworte vorgeschlagen, die teilweise aus „normalen" Worten bestehen und sich daher gut einprägen lassen. Das Kennwort wird nach dem Prinzip „Wort 1 / Ziffernfolge / Sonderzeichen / Wort 2" in einer vorgegebenen Länge zusammengesetzt.
- **Buchstaben und Ziffern:** Zufällige Folgen von Großbuchstaben, Kleinbuchstaben und Ziffern werden zu Kennwortvorschlägen zusammengesetzt.
- **Nur Ziffern:** Zufällige Folgen von Ziffern werden zu Kennwortvorschlägen zusammengesetzt. Diese Konstruktionsprinzip gilt allerdings als nicht so sicher wie andere Verfahren.
- **Zufällig:** Es wird eine völlig zufällige Folge von lateinischen Schriftzeichen zu Kennwortvorschlägen zusammengesetzt.
- **FIPS-181-kompatibel:** Es werden Kennwortvorschläge zusammengestellt, die nach der Durchführungsverordnung *FIPS 181* der Vereinigten Staaten *(Federal Information Processing Standards Publication 181)* berechnet wurden.

Im Feld VORSCHLAG wird der derzeitige Kennwortvorschlag angezeigt. Es handelt sich um eine Kombobox, die Sie aufklappen können, um insgesamt zehn Vorschläge anzeigen zu lassen. Außerdem steht ein Menüpunkt zur Verfügung, um zehn neue Vorschläge berechnen zu lassen. Der Schieberegler LÄNGE erlaubt Ihnen, die gewünschte Länge des neuen Kennworts einzustellen. Sie können zwischen 8 und 31 Zeichen wählen.

Das Feld QUALITÄT stellt mit einem verschieden langen Balken dar, wie hoch die Sicherheit des gerade gewählten Kennworts eingeschätzt wird. Außerdem wechselt der Balken die Farben von rot nach grün, je sicherer das Passwort gilt. Warum ein Kennwort als eventuell unsicher eingestuft wird, wird mit einem Ratschlag wie man es besser machen könnte im Feld TIPP angezeigt.

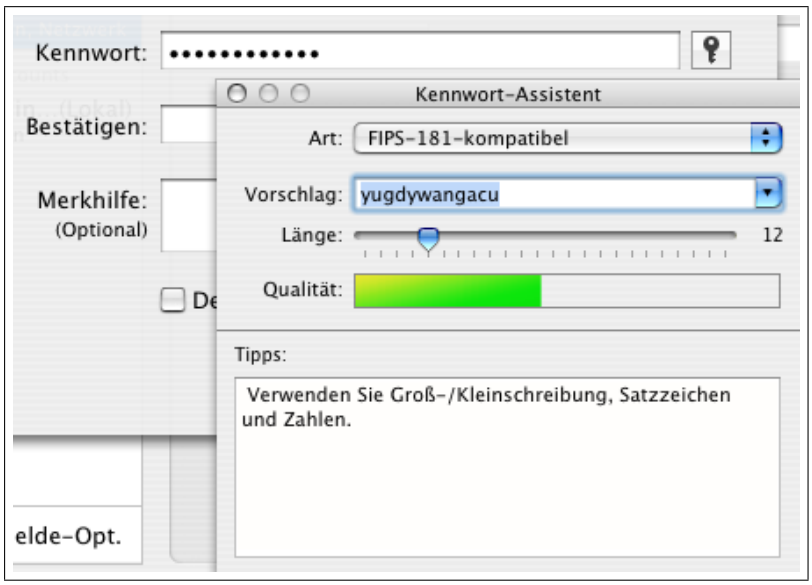

Abbildung 6.8: Der Kennwortassistent ist eine neue Funktion von Mac OS X Tiger, die oft übersehen wird. Der Assistent kann die Sicherheit eines Kennworts einschätzen und selbst gute Kennworte vorschlagen.

6.4 Ausfall der Kerberos-Funktionen in Tiger

Wie erwähnt haben die ersten Versionen von Mac OS X 10.4 Server noch einige Kinderkrankheiten, die sich besonders auf den Startvorgang des Betriebssystems auswirken. Es kann in bestimmten Konfigurationen dazu kommen, dass auch der Kerberos-Schlüsselverteilungsserver nicht startet. Dies ist natürlich besonders kritisch, da alle kerberisierten Dienste im Netzwerk auf die korrekte Funktion des Kerberos-Servers angewiesen sein können. Im schlimmsten Fall kann sich außer den lokalen definierten Benutzern kein Benutzer im Netz mehr anmelden.

Grund für das Versagen der Kerberos-Funktionen ist in den meisten Fällen ein Kommunikationsproblem mit dem DNS-Server beim Start des Betriebssystems. Wenn der DNS-Server auf dem gleichen Computer wie der Kerberos-Server läuft, dann kann es das in Abschnitt 2.7.2 erwähnte Startproblem des DNS-Dienstes sein, das dann in einer Kettenreaktion zum Ausfall von Kerberos und aller anderen Netzdienste führt. Läuft der DNS-Server auf einem Nicht-Tiger-System, können aber auch andere Probleme beim Hochfahren der Netzfunktionen von Tiger dazu führen, dass das Kerberos-Subsystem nicht rechtzeitig mit DNS-Daten versorgt wird und somit den Betrieb einstellt. Ob der Kerberos-Dienst korrekt arbeitet, können Sie in Server-Admin auf der Seite ÜBERSICHT des Dienstes OPEN DIRECTORY prüfen – jedenfalls falls Sie es noch schaffen, das Programm Server Admin zu starten. Wird in der letzten Zeile der Übersicht der Text KERBEROS-STATUS: ARBEITET angezeigt, ist der Betriebszustand in Ordnung. Haben Sie jedoch häufiger Probleme mit dem

Start von Kerberos, so können Sie mit folgender Anleitung versuchen, die Sache in den Griff zu bekommen:

1. Öffnen Sie auf dem Server ein Terminal-Fenster und laden Sie die Datei *hostconfig* über den Befehl `sudo pico /etc/hostconfig` in einen Texteditor.
2. Suchen Sie die Zeile mit dem Schlüsselwort *HOSTNAME*. In der Standardkonfiguration des Servers lautet die entsprechende Konfigurationszeile

   ```
   HOSTNAME=-AUTOMATIC-
   ```

3. Ändern Sie diese Zeile, indem Sie den Eintrag `-AUTOMATIC-` durch den voll qualifizierten DNS-Domänennamen des Servers überschreiben, zum Beispiel

   ```
   HOSTNAME=g4server.example.private
   ```

4. Drücken Sie *ctrl-X* und beantworten Sie den Dialog mit *y* für *yes*, um die Datei zu speichern.
5. Geben Sie den Befehl

   ```
   sudo slapconfig -kerberize diradmin REALM
   ```

   ein. Hierbei muss *diradmin* durch den Kurznamen des Verzeichnisdienstverwalters und *REALM* durch den Namen Ihres Kerberos-Bereichs ersetzt werden.
6. Geben Sie den Befehl

   ```
   sso_util configure -r REALM -f /LDAPv3/127.0.0.1 -a diradmin -p pass -v 1 all
   ```

   ein. Hierbei muss *REALM* durch den Namen Ihres Kerberos-Bereichs, *diradmin* durch den Kurznamen des Verzeichnisdienstverwalters und *pass* durch das Kennwort dieses Verwalters ersetzt werden. Beachten Sie, dass das Kennwort im Klartext auf dem Bildschirm erscheint und im Eingabepuffer des Terminal-Fensters und der History der Shell gespeichert werden.
7. Geben Sie den Befehl

   ```
   sso_util configure -r REALM -f /LDAPv3/127.0.0.1 -a diradmin -p pass -v 1 ldap
   ```

   ein, wobei Sie die gleichen Ersetzungen vornehmen, wie im vorigen Schritt.
8. Starten Sie den Rechner neu.

6.5 Vordefinierte Konten

In der Version 10.4 des Betriebssystems haben sich hinsichtlich der vordefinierten Accounts ein paar Änderungen ergeben. Tabelle 6.1 zeigt die Änderungen bezüglich der Benutzerkonten, Tabelle 6.2 die Änderungen bei den vordefinierten Gruppenkonten. Die Tabellen enthalten nur die Änderungen, die sich gegenüber Panther ergeben haben. Die vollständigen Tabellen sind in Abschnitt 5.5.1 des Hauptbuchs enthalten.

Kurzname	UID	Bedeutung
amavisd	83	Abtrennung der Rechte für SpamAssassin
appowner	87	Mögliche Abtrennung der Rechte für Programme
clamav	82	Abtrennung der Rechte für ClamAV
cyrusimap	77	das frühere Konto *cyrus* hat einen neuen Kurznamen
jabber	84	Abtrennung der Rechte für den iChat-Server
mmuser	-17	dieses Konto ist in Tiger nicht mehr vordefiniert
securityagent	92	Abtrennung der Rechte für privilegierte Operationen
smmsp	25	dieses Konto ist in Tiger nicht mehr vordefiniert
tokend	91	Abtrennung der Rechte für die SmartCard-Verwaltung
windowserver	88	Abtrennung der Rechte für den Window-Server
xgridagent	86	Abtrennung der Rechte für Xgrid-Einzelserver
xgridcontroller	86	Abtrennung der Rechte für die Xgrid-Verwaltung

Tabelle 6.1: Vom System reservierte Benutzerkonten in Mac OS X Tiger. Die Tabelle enthält nur Einträge, die sich gegenüber Panther geändert haben.

6.6 Arbeiten mit Gruppenordnern

In den vergangenen Jahren hat Apple das Arbeiten mit Gruppenordnern immer wieder geändert oder umgestellt. In bestimmten Versionen von Mac OS X funktionieren Gruppenordner schlicht und einfach gar nicht. Wie im Hauptbuch (Abschnitt 5.7.4) beschrieben sind Gruppenordner eigentlich ein Fremdkörper in Mac OS X, da Unix-Systeme üblicherweise nicht mit Gruppenordnern arbeiten. Apple hat jedoch dieses Konzept in Mac OS X eingeführt, um die Funktionalität von Vorgängerprodukten wie *AppleShare IP* wenigstens dem Anschein nach beizubehalten.

Während der Lebensdauer von Panther und für Mac OS X Tiger hat Apple den Umgang mit Gruppenordnern noch einmal genauer dokumentiert. Funktionalität, die ursprünglich automatisch geplant war, wurde teilweise durch Aufrufe auf der Kommandozeile ersetzt. Wir skizzieren im Folgenden das Einrichten eines Gruppenordners auf einem Mac OS X Server.

6.6.1 Einrichten eines Gruppenordners auf einem zentralen Dateiserver

Wir gehen davon aus, dass Sie auf einem Mac OS X Server einen Dateiserverdienst wie AFP aktiviert haben. Es soll nun ein Gruppenordner für die Benutzergruppe *employee* eingerichtet werden. Wir legen diesen Gruppenordner als Unterordner eines zentral freigegebenen Ordners für Gruppenordner an. Apple schlägt in Mac OS X Server den Ordner */Groups*, der im deutschsprachig eingestellten Finder als *Gruppen* angezeigt wird, als übergeordneten Ordner vor.

1. Starten Sie den Arbeitsgruppen-Manager und verbinden Sie sich mit dem

Kurzname	UID	Bedeutung
accessibility	83	Abtrennung der Rechte für Bedienungshilfendienste
amavisd	83	Abtrennung der Rechte für SpamAssassin
appowner	87	Mögliche Abtrennung der Rechte für Programme
authedusers	50	Windows-Gruppe „Angemeldete Benutzer“
certusers	29	Abtrennung der Rechte für Umgang mit Zertifikaten
clamav	82	Abtrennung der Rechte für ClamAV
consoleusers	53	Windows-Gruppe „Terminal-Server-Benutzer“
daemon	1	Abtrennung der Rechte für Unix-Systemdienste
everyone	12	Gruppe zur Abbildung der Windows-Gruppe „Jeder“
group	16	Windows-Gruppe „Erstellergruppe“
interactuser	51	Windows-Gruppe „Interaktiver Benutzer“
jabber	84	Abtrennung der Rechte für den iChat-Server
lp	26	Abtrennung der Rechte für die Druckerverwaltung
mailman	78	Abtrennung der Rechte für die Mailinglisten-Funktion
mysql	74	Abtrennung der Rechte für den MySQL-Datenbankserver
netboot	120	Abtrennung der Rechte für die NetBoot-Funktionen
netusers	52	Windows-Gruppe „Netzwerkbenutzer“
network	69	Windows-Gruppe „Netzwerkkonfigurationsbenutzer“
owner	10	Windows-Gruppe „Eigentümer“
postfix	27	Abtrennung der Rechte für SMTP-Mailserver
qtss	76	Abtrennung der Rechte für QuickTime Streaming Server
securityagent	92	Abtrennung der Rechte für privilegierte Operationen
tokend	91	Abtrennung der Rechte für die Smartcard-Verwaltung
windowserver	88	Abtrennung der Rechte für den Window-Server
xgridagent	86	Abtrennung der Rechte für Xgrid-Einzelserver
xgridcontroller	86	Abtrennung der Rechte für die Xgrid-Verwaltung

Tabelle 6.2: Vom System reservierte Gruppenkonten in Mac OS X Tiger. Die Tabelle enthält nur Einträge, die sich gegenüber Panther geändert haben.

Server, der als Dateiserver für die Gruppenordner arbeiten soll und melden Sie sich als Verzeichnisdienstverwalter an.

2. Wählen Sie in der Symbolleiste den Punkt SHARING.

3. Stellen Sie sicher, dass in der Tabelle NETZWERKORDNER der Ordner *Groups* aufgeführt ist. Ist er das nicht, wechseln Sie in die Tabelle ALLE, navigieren Sie zu *Groups* und kreuzen auf der Karteikarte ALLGEMEIN den Punkt DIESES OBJEKT UND SEINEN INHALT FREIGEBEN an.

4. Prüfen Sie unter dem Bereich PROTOKOLLE, ob die Fileserver-Protokolle, mit denen der Ordner freigegeben wird, nach Ihren Wünschen aktiviert, bzw. deaktiviert sind.

Es sei darauf hingewiesen, dass vollautomatische Mounts für Gruppenordner nicht unterstützt werden, deshalb muss auf der Karteikarte NETZWERKORDNER nichts eingestellt werden. Ein freigegebener übergeordneter Ordner für Gruppenordner ist nun vorhanden. Im nächsten Schritt legen wir den Gruppenordner an und verbinden ihn mit einem Gruppenkonto.

1. Verbinden Sie sich über den Arbeitsgruppen-Manager mit dem Server, auf dem sich das Gruppenkonto befindet, dem ein Gruppenordner zugeordnet werden soll und melden Sie sich als Verzeichnisdienstverwalter an.

2. Wählen Sie in der Symbolleiste den Punkt ACCOUNTS.

3. Wählen Sie in der linken Hälfte des Fensters die Rubrik für Gruppenordner aus und klicken Sie die betreffende Gruppe an.

4. Wechseln Sie in der rechte Hälfte des Fensters zur Karteikarte GRUPPENORDNER.

5. Wenn der freigegebene übergeordnete Ordner mit Standardeinstellungen im Arbeitsgruppen-Manager erstellt wurde, zeigt das Programm bereits einen korrekten Vorschlag für die Netzwerkadresse in der Tabelle an. In Abbildung 6.9 haben wir einen zentralen Gruppenordner und einen zentralen Benutzerordner über das AFP-Protokoll auf dem Server *g4server.example.private* definiert und das Programm schlägt bereits die richtigen Adressen zur Verbindungsherstellung vor. Wenn Sie in der Tabelle den Vorschlag

   ```
   afp://g4server.example.private/Groups
   ```

   anklicken, wird in der Zeile über der Tabelle die letztendlich korrekte Adresse für den Gruppenordner, nämlich

   ```
   afp://g4server.example.private/Groups/employee
   ```

   angezeigt. Der vollständige Pfad entsteht immer dadurch, dass der Langname der Gruppe an den übergeordneten Pfad angehängt wird. Sie können bei Bedarf auch einen neuen Eintrag in der Tabelle manuell erstellen, indem Sie die

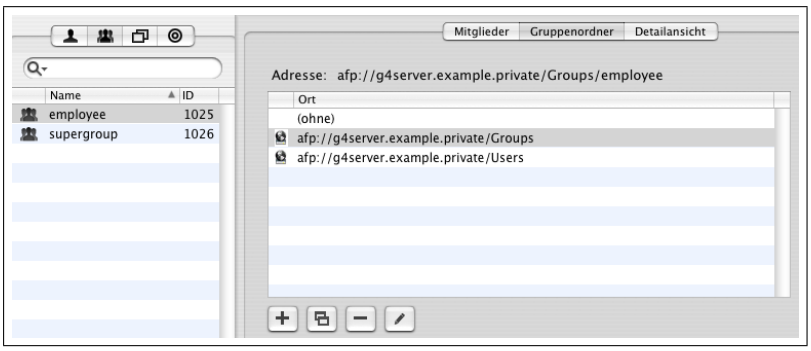

Abbildung 6.9: Ein Gruppenkonto wird im Arbeitsgruppen-Mananger mit einem Gruppenordner verbunden. Wenn Sie die Standardeinstellungen von Apple beibehalten haben, werden die richtigen Einträge bereits vorgeschlagen.

Plus-Schaltfläche unter der Tabelle betätigen. Geben Sie in dem erscheinenden Dialogfenster im oberen Teil unter MAC OS X SERVER / NETZWERKORDNER-URL die Netzwerkadresse des übergeordneten freigegebenen Ordners an und unter PFAD den relativen Teilpfad hierzu (kein führender Schrägstrich), der hinter diese Adresse gehängt wird. Abbildung 6.10 zeigt ein Beispiel.

6. Geben Sie in das Feld EIGENTÜMER im unteren Bereich des Fensters den Kurznamen eines Benutzers an, der im Dateisystem als Eigentümer für den Gruppenordner fungieren soll. Dieser Benutzer wird damit eine Art „Gruppenverwalter“. Sie können die Schaltfläche mit den drei Punkten betätigen, um sich die Liste der Benutzerkonten einblenden zu lassen und einen Eintrag mit der Maus ins Feld zu ziehen.

7. Betätigen Sie die Schaltfläche SICHERN um die Einstellungen abzuspeichern.

Sie können die Schritte des letzten Abschnitts wiederholen, um alle Gruppenordner, die Sie im Moment brauchen, zu definieren. Beachten Sie, dass die Gruppenordner noch gar nicht im Dateisystem existieren. Sie werden nun angelegt.

1. Öffnen Sie ein Terminal-Fenster.

2. Geben Sie das Kommando

   ```
   sudo CreateGroupFolder -v
   ```

   an. Mac OS X erstellt hierdurch alle Gruppenordner, die Sie definiert haben und richtet entsprechende Unterordner mit den richtigen Berechtigungseinstellungen ein. Die Option `-v` bewirkt, dass wir einen ausführlichen Statusbericht erhalten. Durch Hinzufügung des Optionsbuchstabens `-f` können Sie erzwingen, dass Mac OS X auch bei bereits existierenden Ordnern die Berechtigungen noch einmal neu anpasst. Diese Option ist mit Vorsicht zu genießen,

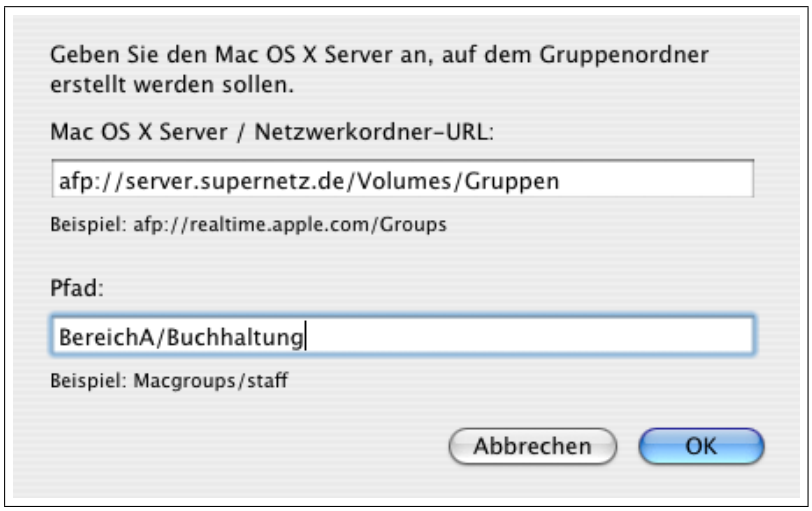

Abbildung 6.10: Haben Sie eine komplexere, angepasste Struktur für die Platzierung von Gruppenordnern angelegt, so können Sie die nötigen Adressdaten manuell eingeben.

da hierbei Sicherheitseinstellungen, die die Gruppenadministratoren eventuell bereits angepasst haben, durch die Standardeinstellungen von Mac OS X überschrieben werden.

6.6.2 Vereinfachung des Zugriffs auf Gruppenordner für die Gruppenmitglieder

Wie erwähnt hat das Anlegen und Definieren eines Gruppenordners keinen weiteren Effekt, außer dass er nun existiert. Möchten die Mitglieder der Gruppe den Ordner verwenden, so müssen sie wissen, auf welchem Server er sich befindet und manuell eine Verbindung herstellen. Dies ist nicht besonders benutzerfreundlich. Mac OS X kann den manuellen Zugriff etwas erleichtern, indem im Dock die richtige Adresse für das Herstellen der Verbindung eingeblendet wird oder ein halbautomatischer Mount zu den Startobjekten der Gruppenmitglieder hinzugefügt wird. Diese Funktionalität wird über verwaltete Einstellungen eingerichtet.

Einblenden eines Symbols für den Gruppenordner im Dock

1. Starten Sie den Arbeitsgruppen-Manager, verbinden Sie sich mit dem Server, der das betreffende Gruppenkonto speichert und melden Sie sich als Verzeichnisdienstverwalter an.

2. Wählen Sie in der linken Hälfte des Fensters das Symbol für Benutzergruppen aus und klicken Sie die betreffende Gruppe an.

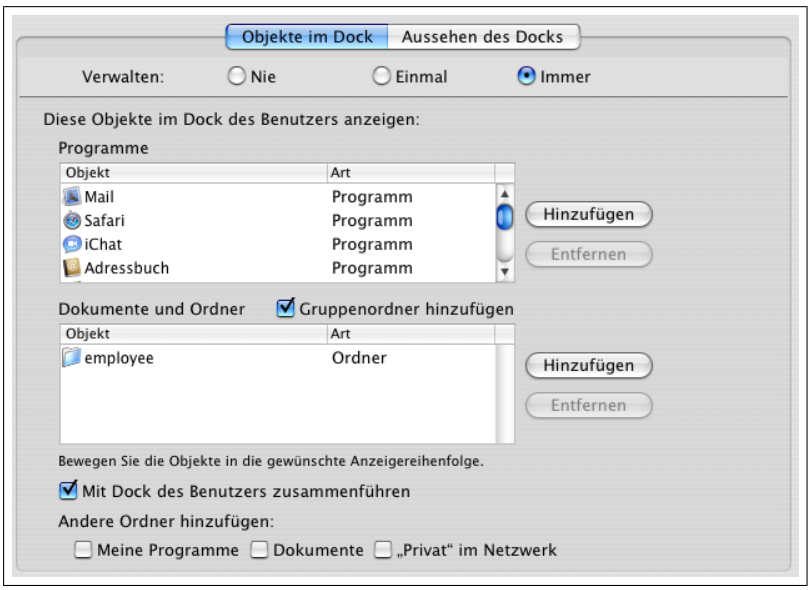

Abbildung 6.11: Über verwaltete Einstellungen ist es möglich, den Mitgliedern der Gruppe ein Symbol für den Gruppenordner im Dock einzublenden. Die Verbindung kann manuell hergestellt werden, ohne dass eine Adresse eingegeben werden muss.

3. Wählen Sie in der Symbolleiste den Punkt EINSTELLUNGEN.
4. Wählen Sie in der Übersicht der Einstellungen die Rubrik DOCK aus.
5. Stellen Sie die Auswahl VERWALTEN auf IMMER.
6. Kreuzen Sie über der unteren Tabelle den Punkt GRUPPENORDNER HINZUFÜGEN an.
7. Betätigen Sie die Schalflächen JETZT ANWENDEN und FERTIG.

Abbildung 6.11 zeigt das Einrichten der verwalteten Einstellung, Abbildung 6.12 das Ergebnis. Beim ersten Start erscheint ein Fragezeichensymbol im Dock. Nach dem Anklicken wird ein Mount-Befehl ausgelöst und das Symbol verwandelt sich in ein Ordnersymbol. Der übergeordnete Gruppenordner erscheint als verbundenes Netzwerk-Volume.

Einrichten eines Startobjekts zum halbautomatischen Mount

1. Starten Sie den Arbeitsgruppen-Manager, verbinden Sie sich mit dem Server, der das betreffende Gruppenkonto speichert und melden Sie sich als Verzeichnisdienstverwalter an.

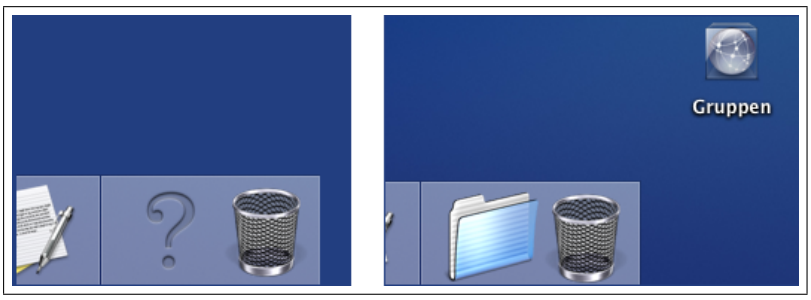

Abbildung 6.12: Vorher und Nachher: Im Dock wird das Symbol zunächst als Fragezeichen angezeigt. Nach Anklicken und Herstellen der Verbindung ist der Gruppenordner verfügbar.

2. Wählen Sie in der linken Hälfte des Fensters das Symbol für Benutzergruppen aus und klicken Sie die betreffende Gruppe an.
3. Wählen Sie in der Symbolleiste den Punkt EINSTELLUNGEN.
4. Wählen Sie in der Übersicht der Einstellungen die Rubrik ANMELDUNG aus.
5. Stellen Sie die Auswahl VERWALTEN auf IMMER.
6. Kreuzen Sie in der unteren Hälfte des Fensters den Punkt GRUPPENVOLUME HINZUFÜGEN an.
7. Betätigen Sie die Schalflächen JETZT ANWENDEN und FERTIG.

In diesem Fall wird die Verbindung zum Gruppenordner unmittelbar nach der Anmeldung hergestellt.

6.7 Verwaltete Benutzerkonten in der Standardversion von Mac OS X

Die Funktionen zum Definieren von Vorgabewerten und Einschränkungen für ein Benutzerkonto wurden in der Standardversion von Mac OS X für Tiger umbenannt: Apple hat sie neu unter dem Stichwort *Kindersicherung* zusammengefasst. Die Funktionalität ist im Wesentlichen die Gleiche, sie ist nur völlig anders gegliedert und es gibt auch einige neue Funktionen.

Wenn Sie im Programm *Systemeinstellungen* unter BENUTZER ein Benutzerkonto ohne Verwalterrechte auswählen, können Sie den neuen Punkt KINDERSICHERUNG aufrufen. Es erscheint eine Tabelle mit fünf Rubriken wie in Abbildung 6.13.

- **Mail:** In der Rubrik MAIL können E-Mail-Adressen aufgelistet werden, mit denen dieser Benutzer Korrespondenz austauschen darf. Zusätzlich kann ei-

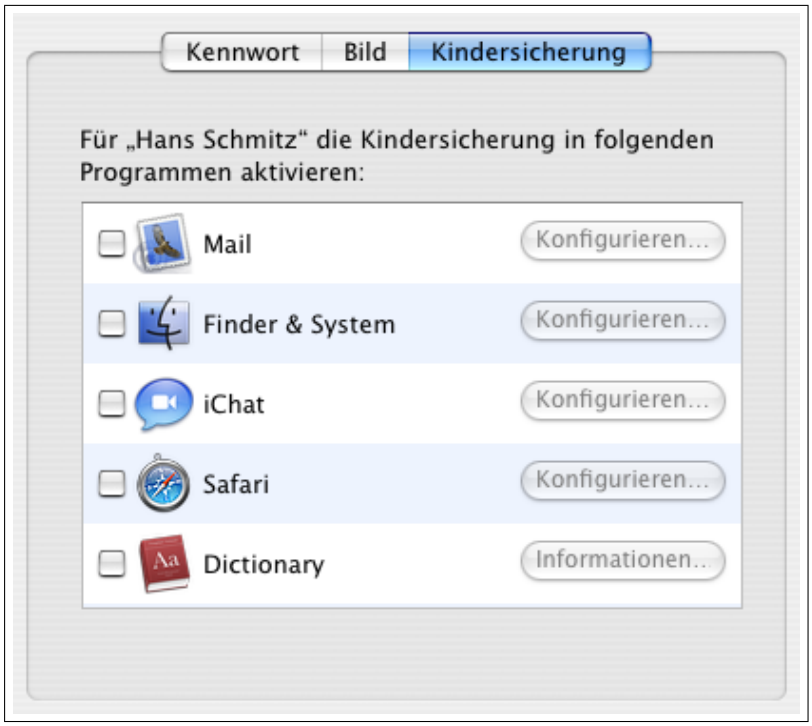

Abbildung 6.13: Die Funktionen zur lokalen Einschränkung von Benutzerkonten wurden komplett neu gestaltet und werden nun als Kindersicherung bezeichnet.

ne bestimmte E-Mail-Adresse festgelegt werden, an die eine „Bitte um Erlaubnis“ geschickt wird, wenn der Benutzer versucht, an eine nicht gelistete Adresse Post zu senden.

- **Finder & System:** Dieser Abschnitt dient als Ersatz für die Funktionen, die Sie früher in Panther unter dem Stichwort EINSCHRÄNKUNGEN gefunden haben. Es lässt sich festlegen, ob ein vollwertiger oder ein eingeschränkter Finder verwendet soll, ob Änderungen an den Einstellungen von Dock, Druckern und anderen Systemeinstellungen zulässig sind, ob optische Medien gebrannt werden dürfen, und welche Programme gestartet werden dürfen. An dieser Stelle sei nochmals daran erinnert, dass es sich hier nicht um die Definition von Zugriffsrechten handelt, sondern nur um einfache Blockademaßnahmen. Benutzer mit Systemkenntnissen könne Wege finden, diese Sperren zu umgehen. Bei Zugriffsrechten wäre dies nicht möglich.

- **iChat:** Ähnlich wie beim Punkt Mail kann hier eine Liste erlaubter Chat-Partner angegeben werden.

- **Safari:** Die Beschränkung von Safari basiert auf einem etwas anderen Prinzip und muss in zwei Schritten durchgeführt werden: Der Systemverwalter muss sich als Erstes als der verwaltete Benutzer anmelden und Safari starten. Innerhalb von Safari kann er dann die Lesezeichen anpassen. Safari wird im Anschluss so eingeschränkt, dass der jeweilige Benutzer nur noch Webseiten aufrufen kann, die über die vorhandenen Lesezeichen erreichbar sind. (Eine vorbereitete Liste von Lesezeichen können erfahrene Verwalter auch durch Ersetzen der Datei *~/Library/Safari/Bookmarks.plist* vorbereiten.) Nach Abmelden und Wiederanmelden als Administrator kann dann für das betreffende Benutzerkonto die Safari-Kindersicherung eingeschaltet werden. Versucht der eingeschränkte Benutzer nun, Internet-Adressen von Domänen aufzurufen, für die keine Lesezeichen vorhanden sind, so erscheint eine Sperre wie in Abbildung 6.14. Natürlich wird auch die Lesezeichen-Liste für Veränderungen gesperrt.

- **Dictionary:** Dieser Punkt kann nur an- und ausgeschaltet werden. Ist er eingeschaltet, kann der Benutzer im englischen Wörterbuch keine Begriffe mehr nachschlagen, die nach Meinung des Herstellers (Oxford University Press) nicht für Kinder geeignet sind.

6.8 Verwaltete Einstellungen für Benutzerkonten

Die verwalteten Einstellungen, die per Open Directory im ganzen Netz verteilt werden können, weisen ebenfalls Änderungen auf. Der frühere Punkt ORTSUNGEBUNDENE ACCOUNTS wurde in MOBILITÄT umbenannt und dessen neue Funktion zur Synchronisation privater mobiler Ordner hatten wir bereits beschrieben. Neu sind auch die Punkte NETZWERK und SOFTWARE-AKTUALISIERUNG. Auf letzteren Punkt gehen wir in Kapitel 14 noch detaillierter ein.

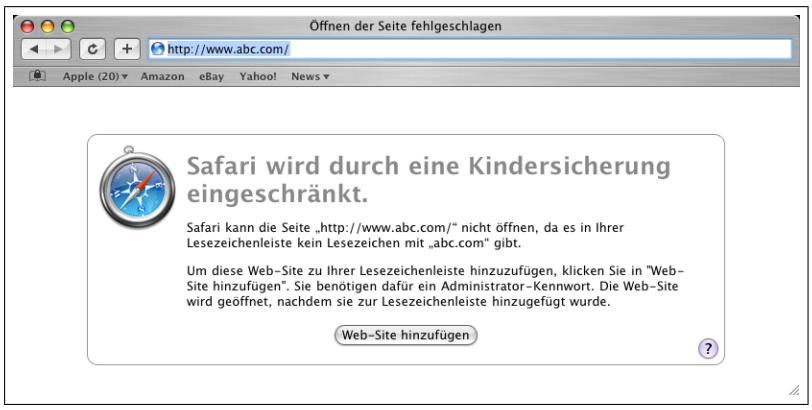
Öffnen der Seite fehlgeschlagen
http://www.abc.com/
Apple (20)
Amazon
eBay
Yahoo!
News
Safari wird durch eine Kindersicherung eingeschränkt.
Safari kann die Seite „http://www.abc.com/" nicht öffnen, da es in Ihrer Lesezeichenleiste kein Lesezeichen mit „abc.com" gibt.
Um diese Web-Site zu Ihrer Lesezeichenleiste hinzuzufügen, klicken Sie in "Web-Site hinzufügen". Sie benötigen dafür ein Administrator-Kennwort. Die Web-Site wird geöffnet, nachdem sie zur Lesezeichenleiste hinzugefügt wurde.
Web-Site hinzufügen

Abbildung 6.14: Aufrufen einer gesperrten Seite in Safari

Zunächst ist zu bemerken, dass auch bezüglich dieser Funktionen Tiger noch einige Kinderkrankheiten aufweist. So lässt sich zum Beispiel in bestimmten Systemkonfigurationen beobachten, dass Client-Computer verwaltete Benutzer immer wieder neu fragen, zu welcher verwalteten Arbeitsgruppe sie sich zuordnen möchten. Auch ist zu beobachten, dass zentral vorgegebene Druckereinstellungen sich immer wieder auf die Klienten vererben, auch wenn diese bereits konfiguriert sind. Wenn Sie ausschließlich PostScript-Drucker in Ihrem Netz haben, fällt die ständige Änderung der Druckerkonfiguration auf den ersten Blick vielleicht gar nicht auf, da alle Drucker dann weitgehend miteinander kompatibel sind. Das Öffnen einer Druckerauswahlliste kann aber zur großen Überraschung werden, wenn alle Drucker plötzlich doppelt und dreifach auftauchen und nur als generische Standarddrucker konfiguriert sind. Sie sollten in diesem Fall der Sache nachgehen und das Verwalten der Druckereinstellungen wenn nötig abschalten, bis Apple das Problem in den Griff bekommen hat.

Wenn Sie ein Benutzer-, Gruppen- oder Computerlistenkonto im Arbeitsgruppen-Manager auswählen und in der Symbolleiste EINSTELLUNGEN anklicken, wird Ihnen zunächst eine erweiterte Legende am unteren Bildrand auffallen. Wenn Sie *mehrere* Konten im linken Teil des Fensters auswählen, unterscheidet die grafische Darstellung nun durch ein dunkelgrau oder hellgrau markiertes Pfeilsymbol, ob alle, bzw. nur ein Teil der ausgewählten Konten von verwalteten Einstellungen betroffen sind (Abbildung 6.15).

Der Auswahlknopf DETAILS ist komplett neu: Mit ihm ist es zum einen möglich, genau nachzuvollziehen, was innerhalb von Mac OS X technisch geschieht, sobald Sie eine verwaltete Einstellung aktivieren, zum anderen können Sie damit auch Einstellungen beliebiger Drittanbieterprogramme verwalten, also Vorgaben für eigene Programme definieren, die Apple standardmäßig nicht vorgesehen hat. Dieses Funktionsmerkmal erfordert zwar im Einzelfall technische Kenntnisse über die Art und Weise wie in Mac OS X Programmeinstellungen gespeichert werden, kann sich aber als sehr hilfreich erweisen: Sie können nun einen kompletten Vorgabensatz für alle in Ihrem Netz installierten Programme definieren, so dass jeder neu hinzu-

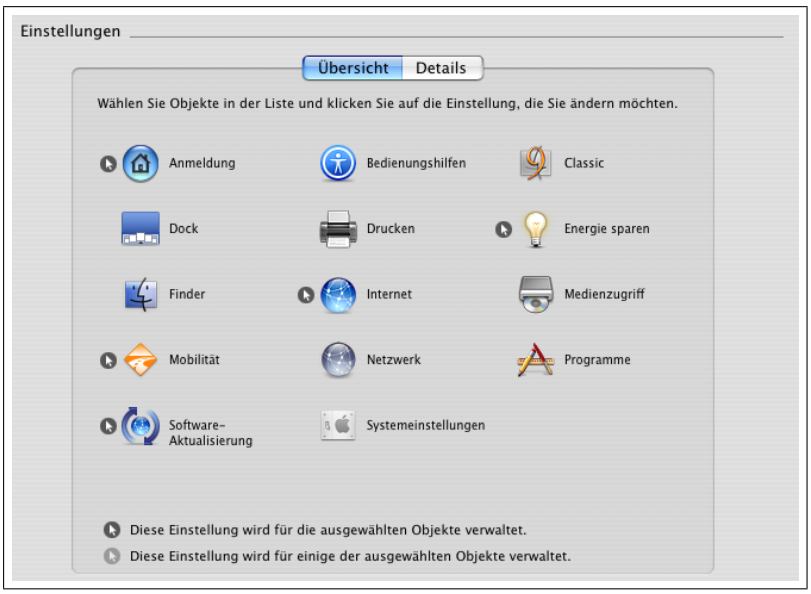

Abbildung 6.15: Die verwalteten Einstellungen im Arbeitsgruppen-Manager weisen einige Neuerungen gegenüber Panther auf.

kommende Benutzer beim ersten Anmelden eine optimal auf Ihre Gegebenheiten zugeschnittene Umgebung mit den richtigen Einstellungen für alle Programme vorfindet.

6.8.1 Einrichten von Einstellungen für nicht unterstützte Programme

Technische Grundlagen

Um Einstellungen für vom Arbeitsgruppen-Manger nicht direkt unterstützte Programme verwalten zu können, ist es notwendig, einen kurzen Blick darauf zu werfen, wie das „Verwalten“ von Einstellungen intern abläuft. Wie Sie vielleicht wissen, speichert Mac OS X die Einstellungen von Programmen immer im Unterordner

```
Library/Preferences
```

desjenigen Zuständigkeitsbereichs, auf den sich die Einstellungen beziehen. Bei benutzerbezogenen Einstellungen wird der entsprechende Unterordner im Privatordner des Benutzers verwendet, computerbezogene Einstellungen, die für alle Benutzer eines Computers gelten, werden im Wurzelordner, also */Library/Preferences* gespeichert. Denkbar wäre auch eine netzweite Speicherung von Einstellungen im Ordner */Network/Library/Preferences*, was im Moment jedoch von Mac OS X noch nicht unterstützt wird.

Zur Speicherung der Einstellungen wird eine speziell eingeschränkte Form von *Mac OS X Property Lists*, also dem Standardformat von Mac OS X zur Speicherung von Eigenschaftslisten verwendet. Eigenschaftslisten sind Datenstrukturen, die aus einer Aufreihung von Werten bestehen, wobei diese Werte entweder in einer bestimmten Sortierung oder mit zusätzlichen Schlüsselnamen versehen gespeichert sind. Als Werte sind Zahlen, Texte, Ja/Nein-Werte, Bytefolgen oder beliebig verschachtelte Folgen dieser Werte erlaubt. Die entsprechenden Dateien tragen das Suffix *.plist*, wobei zwischen vollwertigen Property Lists und Einstellungsdateien im Suffix nicht unterschieden wird. Der Dateiname vor der plist-Endung muss bei Einstellungsdateien nach einem speziellen Prinzip aufgebaut sein, das man als *Globally Unique Naming* (weltweit eindeutige Benennung) bezeichnet. Hierbei verwendet man ähnlich wie beim DNS-Namensschema hierarchisch durch Punkte getrennte Namensteile, anders als bei DNS jedoch in der „richtigen" Reihenfolge, von der obersten zu den unteren Hierarchieebenen von links nach rechts. Apple schreibt vor, dass zunächst der entsprechend umgedrehte DNS-Domänenname des Programmherstellers und danach eine hierarchisch gegliederte Beschreibung der Einstellungen im Dateinamen genannt werden muss. Dieses Benennungsverfahren garantiert, dass jede Einstellungsdatei für jedes Programm einheitlich ist und niemals zwei Hersteller zufällig den gleichen Namen für ihre Einstellungen wählen. Ein Programm kann so niemals versehentlich die Einstellungen eines anderen Programms überschreiben.

Im einfachsten Fall wird nur der Programmname an die DNS-Domäne angehängt, zum Beispiel

```
com.apple.Safari.plist
```

für die Einstellungsdatei *Safari* des Herstellers mit der DNS-Domain *apple.com*. Aber auch tiefer verschachtelte Hierarchieebenen wie

```
com.apple.quicktime.plugin.preferences.plist
com.apple.speech.recognition.feedback.prefs.list
```

sind nicht unüblich. Jeder dieser Namen bezeichnet eine sogenannte *Einstellungsdomäne*. Für das Dock ist zum Beispiel die Einstellungsdomäne *com.apple.dock* zuständig, deren Inhalt in einem oder mehreren Preferences-Ordnern jeweils unter dem Namen *com.apple.dock.plist* abgespeichert ist.

Die Einstellungsdateien können mit Apples Programm *Property List Editor* angezeigt und verändert werden. Ist Mac OS X mitsamt der Entwicklerumgebung Xcode installiert worden, so befindet sich der Editor an der Position

/Developer/Applications/Utilities/Property List Editor.app.

Das gleiche Programm befindet sich aber auch im Paket mit den Administrations-Tools von Mac OS X Server. Sie finden es in der von Apple herunterladbaren DMG-Datei im Ordner *Utilities*.

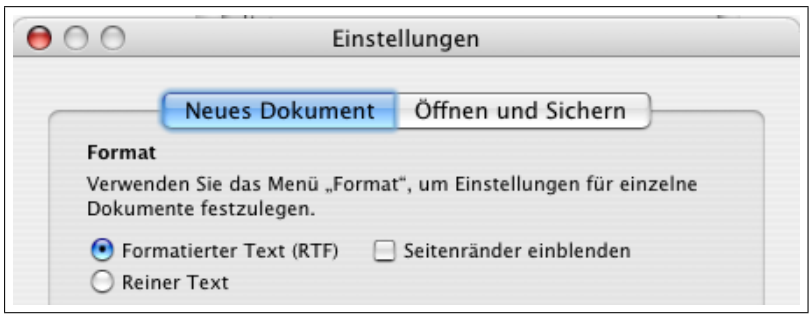

Abbildung 6.16: Die Vorgabe für das Textformat neuer Dokumente in TextEdit ist ein Beispiel, wie Programme Einstellungen in Mac OS X speichern.

Es sei darauf hingewiesen, dass Mac OS X alle diese Dateien anlegt, nicht etwa die Programme selbst! (Es gibt leider einige schlecht programmierte Produkte von Drittanbietern, die tatsächlich selbständig Dateien in *Library/Preferences* anlegen. Das ist allerdings die Ausnahme und verstößt klar gegen Apples Design-Richtlinien für Mac OS X.) Wenn ein Programm einen Einstellungswert speichern oder ändern möchte, ist die korrekte Vorgehensweise, dass das Programm ein Kommando der Form „halte für den Zuständigkeitsbereich B und die Einstellungsdomäne D einen Einstellungswert W unter dem Namen N fest“ an Mac OS X übergibt. Das Betriebssystem merkt sich dann den neuen Wert W, und zwar zunächst nur im Hauptspeicher. Spätestens wenn das laufende Programm beendet wird, wird der neue Wert dauerhaft in einer plist-Datei der Domäne D abgespeichert, worum sich Mac OS X völlig selbständig kümmert. Läuft das Programm später wieder, fragt es Mac OS X „gibt es eine Einstellung, die mit dem Namen N für die Domäne D im Zuständigkeitsbereich B gespeichert ist?“. Falls ja übernimmt das Programm diese Einstellung.

Schauen wir uns dies noch einmal im konkreten Beispiel an. Das Programm *TextEdit* verwendet beispielsweise einen Einstellungswert, in dem es speichert, ob neue Textfenster wahlweise in der Betriebsart „formatierter Text“ oder in der Betriebsart „Reiner Text“ geöffnet werden sollen. Im ersten Fall verhält sich das entsprechende Textfenster wie ein Textverarbeitungsprogramm, in letzterem Fall wie ein Texteditor. Wenn Sie diese Vorgabe im Fenster EINSTELLUNGEN von TextEdit vornehmen (siehe Abbildung 6.16), führt dies letztendlich dazu, dass Mac OS X einen geänderten Wert in TextEdits Einstellungsdatei abspeichert.

Wenn Sie einen Blick in den privaten Ordner *Library/Preferences* eines Benutzers werfen, der TextEdit bereits genutzt und Einstellungen geändert hat, werden Sie feststellen, dass eine Datei mit dem Namen *com.apple.TextEdit.plist* vorhanden ist. Dies muss die Einstellungsdatei von TextEdit sein. Öffnen Sie die Datei im Property List Editor, und klappen Sie die enthaltene Eigenschaftsliste auf, so erhalten Sie eine Liste mit einer Vielzahl von Einstellungswerten (Abbildung 6.17). Jeder Wert ist mit einem eindeutigen Namen versehen. Diese Namen sind in der linken Spalte aufgelistet und werden vom jeweiligen Programm frei vergeben. Leider ist in der

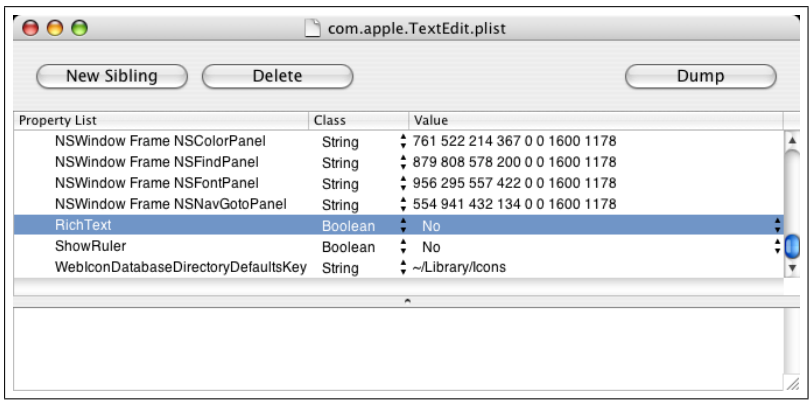

Abbildung 6.17: Einstellungsdaten werden von Mac OS X vollautomatisch in Property List-Dateien abgelegt. Die Vorgabe für das Standardformat von TextEdit schlägt sich beispielsweise unter der Eigenschaft mit dem Namen *Rich Text* nieder.

Regel nirgendwo festgehalten, welcher Name sich auf welche Einstellung bezieht, aber mit etwas Spürsinn und guten Englischkenntnissen lässt sich oft erraten, was unter den einzelnen Namen abgespeichert ist.

Die von uns beschriebene Wahlmöglichkeit für die Betriebsart „formatierter Text" ist unter dem Namen *Rich Text* gespeichert. Der Hinweis BOOLEAN in der zweiten Spalte CLASS gibt an, dass es sich um einen Ja/Nein-Wert handelt. In der dritten Spalte VALUE ist schließlich der aktuelle Wert zu finden. Er lautet in diesem Falle NO, wenn TextEdit neue Fenster *nicht* in der Betriebsart „formatierter Text" öffnen soll und YES, wenn dies der Fall ist. Beachten Sie, dass der Eintrag RICH TEXT auch komplett fehlen darf. Das hat zur Folge, dass das Programm keine vom Benutzer eingestellte Vorgabe, sondern den vom Programmhersteller in das Programm eingebauten Standardwert verwendet.

Angenommen der Benutzer mit dem Account *hans* schaltet durch Drücken des Knopfes REINER TEXT in Abbildung 6.16 die Einstellung von TextEdit um. In diesem Fall sendet TextEdit intern das Kommando „halte für den Zuständigkeitsbereich *Benutzer hans* und die Einstellungsdomäne *com.apple.TextEdit* den Wert *No* für die Einstellung mit dem Namen *Rich Text* fest". Zu einem von Mac OS X gewählten Zeitpunkt, spätestens jedoch beim Beenden von TextEdit, ändert Mac OS X die Einstellungsdatei, die sich in unserem Beispielnetz an der Stelle

/Network/Servers/g4server/Users/hans/Library/Preferences/com.apple.TextEdit.plist

befindet, so ab, dass die neue Vorgabe gespeichert wird. Durch dieses Beispiel bekommen Sie eine ungefähre Vorstellung, wie Mac OS X alle Einstellungen im Hintergrund verwaltet. Doch wie läuft das Ganze ab, wenn es sich um eine *verwaltete* Einstellung handelt?

6.8.2 Die Realisierung verwalteter Einstellungen

Im Prinzip findet nur ein zusätzlicher Schritt statt, der unmittelbar nach dem Anmeldevorgang eines verwalteten Benutzers ausgeführt wird. Das Programm *loginwindow*, das das Anmeldefenster anzeigt und auch die komplette Verwaltung des Anmeldevorgangs übernimmt, fragt beim System nach, ob für diesen Benutzer entweder in der lokalen Kindersicherung oder in der Open Directory-Datenbank verwaltete Einstellungen enthalten sind. Falls ja, dann wird noch vor dem Start irgendeines Programms der betreffende Einstellungswert dieses Benutzers *mit dem verwalteten Einstellungswert überschrieben.* Das ist im Prinzip der ganze Trick. Auf diese Weise werden dem Benutzer die gewünschten Einstellungen vorgegeben.

In Wirklichkeit ist der Vorgang etwas komplizierter, da Mac OS X die verwalteten Einstellungen in einem Zwischenspeicher (Cache-Dateien) ablegt, damit nicht bei jedem Anmeldevorgang ein aufwändiger Abgleich über Open Directory erforderlich ist. Weiterhin ist Mac OS X auch in der Lage, verwaltete Einstellungen zu schützen, also zu verhindern, dass der Benutzer die Einstellung während der laufenden Anmeldesitzung ändert. Diese Details spielen aber für die weitere Betrachtung keine Rolle.

Die verwalteten Einstellungen sind nach dem gleichen Ablageprinzip wie die normalen Einstellungen gespeichert. Einziger Unterschied ist, dass sie sich an einem speziellen Ablageort für verwaltete Einstellungen befinden und die benannten Einstellungswerte zusätzlich noch in die Kategorien

- EINMAL: nur beim ersten Anmeldevorgang überschreiben,
- HÄUFIG: bei jedem Anmeldevorgang überschreiben, aber während der Benutzersitzung Änderungen zulassen,
- IMMER: bei jedem Anmeldevorgang überschreiben und die Einstellung für den Benutzer sperren

unterteilt sind. Wie dies im einzelnen abläuft, können Sie sehen, indem Sie im Arbeitsgruppen-Manager bei den verwalteten Einstellungen die neue Rubrik DETAILS auswählen (Abbildung 6.18).

Die Karteikarte DETAILS enthält eine dreispaltige Tabelle mit allen verwalteten Einstellungen des gerade angewählten Accounts. In der ersten Spalte wird der übliche Markierungspfeil angezeigt, der symbolisiert, ob in der jeweiligen Zeile Einstellungen wirksam werden, die für die gerade ausgewählten Konten gültig sind. Die zweite Spalte enthält die Namen der Komponenten, für die die Einstellungen gelten, die dritte Spalte den Namen der Einstellungsdomäne. In vielen Fällen ist der Inhalt der zweiten und dritten Spalte gleich, nämlich dann, wenn Mac OS X der Domäne nicht eindeutig einen bestimmten Namen zuordnen konnte. Hierzu später mehr.

Haben Sie bereits verwaltete Einstellungen über die Karteikarte ÜBERSICHT definiert, so spiegelt sich deren Definition unter DETAILS wider. In der Regel wird zum Beispiel für die Domäne *com.apple.mcx* ein Eintrag definiert sein: Es handelt sich hierbei um die Verwaltung der Einstellung der verwalteten Einstellungen.

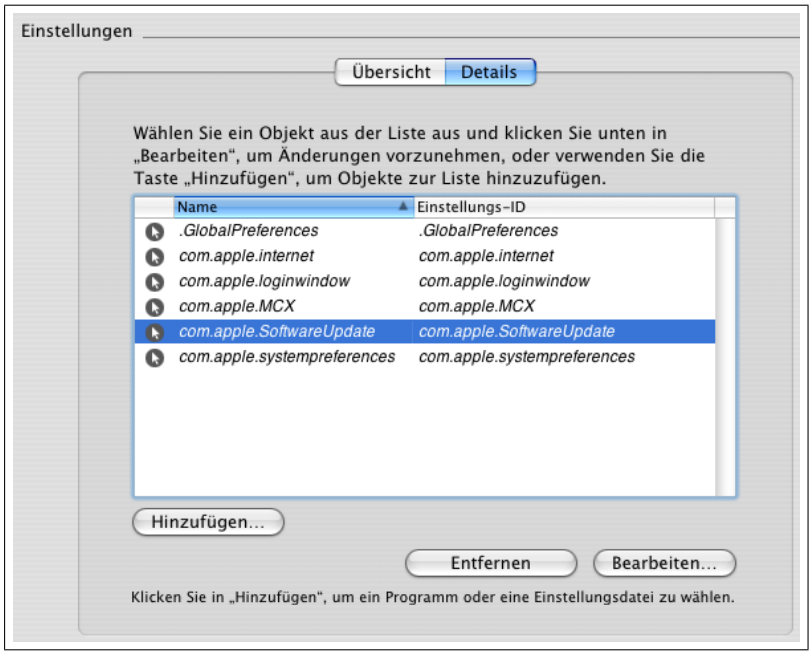

Abbildung 6.18: Wie Mac OS X intern mit den verwalteten Einstellungen umgeht, lässt sich mit der neuen Funktion DETAILS feststellen. Sie kann genutzt werden, um Voreinstellungen für beliebige Drittanbieterprogramme zu definieren.

Angenommen wir möchten das Programm TextEdit aus unserem vorangegangenen Beispiel nun so einrichten, das auf einer bestimmten Liste von Computern TextEdit grundsätzlich mit der Voreinstellung „neue Dokumente werden als reiner Text angelegt" betrieben werden soll. Dies ist ein durchaus praxisnahes Beispiel, es könnte sich zum Beispiel um Computer in einem Büro oder Klassenraum handeln, wo TextEdit hauptsächlich zur Programmentwicklung, nicht zur Textverarbeitung eingesetzt wird. Wir erinnern uns: Hierzu müssen wir in der Einstellungsdomäne *com.apple.TextEdit* die Eigenschaft mit dem Namen *Rich Text* auf den logischen Wert *No* setzen.

1. Starten Sie TextEdit und öffnen Sie den Menüpunkt TEXTEDIT | EINSTELLUNGEN.
2. Stellen Sie im Einstellungsfenster beim Absatz FORMAT die Einstellung auf REINER TEXT um (siehe auch Abbildung 6.16).
3. Beenden Sie TextEdit.
4. Sorgen Sie dafür, dass der Arbeitsgruppen-Manager läuft und Sie mit einem gültigen Kennwort am Verzeichnisknoten angemeldet sind, der die betreffenden Konten enthält.
5. Wählen Sie in der linken Hälfte des Fensters die gewünschten Konten (Benutzer, Gruppen oder Computerlisten) aus.
6. Klicken Sie in der Symbolleiste den Punkt EINSTELLUNGEN an.
7. Wählen Sie in der rechten Hälfte des Bildes die Rubrik DETAILS aus.
8. Drücken Sie unterhalb der Tabelle den Knopf HINZUFÜGEN. . . .
9. Es erscheint ein gleitendes Dialogfenster zum Öffnen von Dateien. Wählen Sie das Programm *TextEdit* im Programme-Ordner von Mac OS X aus, wobei die Option EINSTELLUNGEN DES PROGRAMMS IMPORTIEREN eingeschaltet bleiben sollte.

Danach erscheint ein neuer Eintrag für die Domäne *com.apple.TextEdit* in der Tabelle. Beachten Sie, dass Mac OS X automatisch aus dem ausgewählten Programm bestimmt hat, wie die Einstellungsdomäne des jeweiligen Programms lautet. Wenn Sie den Namen bereits wissen, hätten Sie im Dialogfenster übrigens auch direkt die plist-Datei aus Ihrem (oder einen fremden) Preferences-Ordner von TextEdit auswählen können.

Beim Anlegen der neue Eintragung hat der Arbeitsgruppen-Manager automatisch alle derzeitigen Einstellungen des Programms TextEdit aus Ihrem derzeitigen Benutzerkonto, bzw. aus der plist-Datei, die Sie ausgewählt hatten, in die Kategorie *Häufig* der verwalteten Einstellungen übertragen. Dies ist eine hilfreiche Komfortfunktion, Sie können so ein bestimmtes Benutzerkonto als „Musterbenutzer" einrichten und dessen plist-Dateien als Basis für die verwalteten Einstellungen übernehmen. Oft ist es aber zuviel des Guten: Einige Einstellungen – zum Beispiel die

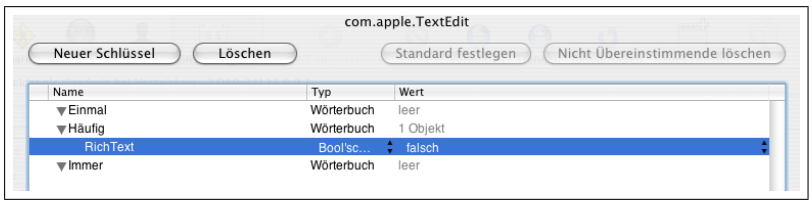

Abbildung 6.19: Wir definieren eine verwaltete Einstellung für TextEdit. Über die manuelle Vorgabe von Eigenschaftslisten lassen sich auch Programme, die im Arbeitsgruppen-Manager nicht vorgesehen sind, mit verwalteten Einstellungen versehen.

Liste der zuletzt geöffneten Dateien, die immer auch in den plist-Dateien abgespeichert ist – sollten nicht unbedingt als Vorlage für die verwalteten Einstellungen dienen. In unserem Beispiel wollen wir ausschließlich die Einstellung *Rich Text* auf *No* setzen, alle anderen Werte sollen so bleiben wie sie sind. Falls Sie im aktuellen Benutzerkonto TextEdit noch nie benutzt hatten, ist die Einstellung, die wir gerade eben geändert hatten, die einzige Einstellung und es stimmt bereits alles. Hatten Sie aber TextEdit in der Vergangenheit bereits benutzt, so müssen wir die überflüssigen Einstellungen, die nicht als Vorlage dienen sollen, löschen.

1. Wählen Sie die Zeile COM.APPLE.TEXTEDIT in der Tabelle aus und drücken Sie den Knopf BEARBEITEN... rechts unter der Tabelle.
2. Es erscheint eine Übersicht mit den Kategorien EINMAL, HÄUFIG, IMMER. Klappen Sie den Punkt HÄUFIG mit dem nebenstehenden Dreieck auf.
3. Suchen Sie die Einstellung RICH TEXT und prüfen Sie, ob sie tatsächlich auf *No* steht. Die deutsche Fassung des Arbeitsgruppen-Managers übersetzt diesen Wert mit dem Begriff FALSCH.
4. Falls unter dem Namen HÄUFIG noch andere Einstellungen außer RICH TEXT enthalten sein sollten, wählen Sie diese Zeilen aus und betätigen Sie den Knopf LÖSCHEN. Wiederholen Sie diesen Vorgang, bis RICH TEXT der einzige Eintrag im Bereich HÄUFIG ist (Abbildung 6.19).
5. Drücken Sie den Knopf FERTIG unterhalb der Tabelle.

Wenn sich nun ein Benutzer im Netzwerk anmeldet und sein Konto befindet sich unter den Benutzer-, Gruppen- oder Computerlistenkonten, die Sie ausgewählt hatten, wird sein Einstellungswert für neue Dokumente in TextEdit wie gewünscht auf die Betriebsart *Reiner Text* umgestellt. Nach dem gleichen Prinzip können Sie für beliebige Programme Voreinstellungen in Ihrem Netz definieren. Die einzige Voraussetzung ist, dass es sich um native Mac OS X-Programme handeln muss. Für einige Altlastenprogramme, die noch aus der klassischen Mac OS-Welt stammen, geht dies nicht, da dort die Programme sich noch selbst um Einstellungen kümmern mussten und Mac OS X somit keine Kontrolle hat, wie ein solches Programm seine Einstellungen verwaltet.

Wenn Sie die Vorgaben für eine Einstellungsdomäne im Arbeitsgruppen-Manager geöffnet haben, können Sie auch die Schaltfläche NEUER SCHLÜSSEL betätigen, um selbständig einen Eintrag neu anzulegen. Voraussetzung ist natürlich, dass Sie den Namen dieser Einstellung und deren Datentyp (Zeichenkette, Wörterbuch, Array, Ganzzahl, Fließkommazahl, Bool'scher Wert, Datum, Daten, Alias, URL) wissen müssen. Dies ist ein Nachteil, den Programme mit einem sogenannten *Einstellungsmanifest* abstellen können.

6.8.3 Arbeiten mit Einstellungsmanifesten

Die vorgestellte Technik zum Definieren von verwalteten Einstellungen ist sehr leistungsstark, erfordert aber einige technische Kenntnisse über ein Programm. Den Namen der Einstellungsdomäne kann der Arbeitsgruppen-Manager noch selbst herausfinden, bei den Namen der Einstellung selbst und deren Datentyp ist dies jedoch unmöglich, da diese Angaben vom jeweiligen Programm völlig frei definiert werden können und es keinen Weg gibt, diese Daten aus einem vorhandenen Programm zu ermitteln. Bis jetzt haben wir uns nur eine vorhandene Präferenzendatei mit dem Property List Editor angeschaut und versucht zu „erraten", was die einzelnen Einstellungen bedeuten. Einstellungen, die noch nie geändert wurden, sondern noch auf dem Standardwert stehen, schlagen sich gar nicht in der plist-Datei nieder.

Um diesen Mangel beheben zu können, gibt Apple den Programmen ab Mac OS X Tiger die Möglichkeit, ihre Einstellungen in einer zusätzlichen Datei freiwillig aufzulisten und zu beschreiben. Eine solche Datei wird *Einstellungsmanifest* genannt. Sie können sich ein solches Manifest wie einen Lieferschein oder eine Art Lexikon vorstellen, das

- alle Einstellungen auflistet, bei denen es sinnvoll sein könnte, sie als verwaltete Einstellungen zu nutzen,
- den richtigen Datentyp für diese Einstellung angibt,
- in natürlicher Sprache beschreibt, wozu diese Einstellung dient, und
- beschreibt, welche Bedeutung die Werte der Einstellung haben und wie sie interpretiert werden.

Es sei betont, dass ein solches Manifest freiwillig ist. Im Moment gibt es nur sehr, sehr wenige Anbieter, die ihre Programme mit Einstellungsmanifesten ausstatten. Auch in Mac OS X selbst werden die Manifeste bis jetzt nur an wenigen Stellen eingesetzt. Sie können wie folgt feststellen, ob ein Programm ein Einstellungsmanifest besitzt:

1. Wählen Sie das Symbol des Programms im Finder aus.
2. Öffnen Sie über die rechte Maustaste (oder ctrl-Klick) das Kontextmenü und wählen Sie den Punkt PAKETINHALT ZEIGEN aus.

3. Navigieren Sie in den Unterordner *Contents*/*Resources*.
4. Suchen Sie nach Dateien mit dem Suffix *.manifest*, bzw. mit der Art *Managed Preference Manifest*. Diese Dateien tragen üblicherweise den Namen der Einstellungsdomäne.

Wenn Sie keine solche Datei finden, dann hat dieses Programm kein Manifest. Die Tiger-Version von Safari wird beispielsweise mit einem Einstellungsmanifest geliefert. Sie finden es an der Position

```
/Applications/Safari.app/Contents/Resources/com.apple.Safari.manifest/
```

Das Manifest von Safari ist besonders interessant, weil es sich gleich auf zwei Einstellungsdomänen bezieht. Safari verwendet nämlich die Domäne

```
com.apple.Safari
```

für die Einstellungen des eigentlichen Programms und

```
com.apple.WebFoundation
```

für die Betriebssystemfunktionen, die die HTML-Dokumente interpretieren und im Fenster von Safari darstellen. Wir zeigen am Beispiel von Safari, wie man mit einem solchen Manifest arbeitet:

1. Stellen Sie wie im letzten Beispiel sicher, dass das Programm Safari im aktuellen Benutzerkonto mindestens einmal aufgerufen wurde, so dass Einstellungen vorhanden sind.
2. Sorgen Sie dafür, dass der Arbeitsgruppen-Manager läuft und Sie mit einem gültigen Kennwort am Verzeichnisknoten angemeldet sind, der die Konten enthält, für die verwaltete Einstellungen definiert werden sollen.
3. Wählen Sie in der linken Hälfte des Fensters die gewünschten Konten (Benutzer, Gruppen oder Computerlisten) aus.
4. Klicken Sie in der Symbolleiste den Punkt EINSTELLUNGEN an.
5. Wählen Sie in der rechten Hälfte des Bildes die Rubrik DETAILS aus.
6. Drücken Sie unterhalb der Tabelle den Knopf HINZUFÜGEN....
7. Es erscheint ein gleitendes Dialogfenster zum Öffnen von Dateien. Wählen Sie das Programm *Safari* im Programme-Ordner von Mac OS X aus.

Bei einem Programm mit Manifest bekommt das Ankreuzfeld EINSTELLUNGEN DES PROGRAMMS IMPORTIEREN nun eine entscheidende Bedeutung: Ist das Feld nicht angekreuzt, übernimmt der Arbeitsgruppen-Manager nur das Manifest und Sie können danach mit einer leeren Schablone für das Programm beginnen, bestimmte

Einstellungen vorzudefinieren. Ist das Feld dagegen angekreuzt, übernimmt der Arbeitsgruppen-Manager Manifest *und* die derzeitigen Einstellungen aus der plist-Datei des aktuellen Benutzers, um sie als Vorlage zu verwenden. Haben Sie die oben skizzierten Schritte durchgeführt, so werden zwei neue Einträge mit dem Namen *Safari* in der Tabelle angelegt.

1. Wählen Sie nun den Eintrag mit der Einstellungs-ID *com.apple.Safari* in der Tabelle aus und drücken Sie auf BEARBEITEN. . . .
2. Es erscheint das bekannte Dialogfenster zum Editieren der Eigenschaftswerte. Haben Sie Einstellungen aus dem Benutzerkonto übernommen, so sind Werte in der Rubrik HÄUFIG vorhanden. Haben Sie keine Einstellungen importiert, so sind alle drei Rubriken leer. Wählen Sie nun die Rubrik HÄUFIG aus, indem Sie die Zeile anklicken und danach das Aufklappdreieck anklicken.
3. Betätigen Sie die Schaltfläche NEUER SCHLÜSSEL.
4. Der Arbeitsgruppen-Manager legt einen neuen Leereintrag mit dem Namen NEUES OBJEKT an. Eine orangefarbene Markierung warnt, dass *Neues Objekt* kein gültiger Name für eine Einstellung ist, da dieser Name nicht im Manifest enthalten ist. Klicken Sie nun auf die neben dem Namen stehenden kleinen Pfeilsymbole. Sie erhalten ein Menü, das in deutscher Sprache alle interessanten Einstellungsmöglichkeiten von Safari beschreibt (Abbildung 6.20).

Sie können nun beispielsweise die Einstellung BILDER ANZEIGEN auswählen. Der Datentyp wechselt hierdurch sofort auf BOOL'SCHER WERT und es wird der Standardwert WAHR vorgeschlagen. Möchten Sie Ihren Netzwerkbenutzer verbieten, dass Safari Bilder anzeigt, so könnten Sie diesen Wert auf FALSCH umstellen.

- Durch Anklicken der Schaltfläche STANDARD FESTLEGEN stellt der Arbeitsgruppen-Manager für die gerade ausgewählte Einstellung einen Wert ein, der dem vom Programm definierten Standardwert entspricht.
- Haben Sie aus einer plist-Datei Einstellungen importiert, die das Manifest als „nicht sinnvoll für eine Voreinstellung" beschreibt – wie beispielsweise die Liste der zuletzt geöffneten Dateien – so können Sie alle diese außerhalb des Manifests liegenden Voreinstellungen auf einen Schlag durch Drücken der Taste NICHT ÜBEREINSTIMMENDE LÖSCHEN entfernen. Die orangefarbenen Warnmarkierungen werden entsprechend verschwinden.

6.9 Einstellungen für den Netzwerkordner des Finders

6.9.1 Einführung

Eine weitere neue Funktion von Mac OS X Tiger besteht darin, dass Sie über eine besondere verwaltete Einstellung steuern können, wie der *Netzwerkordner* im

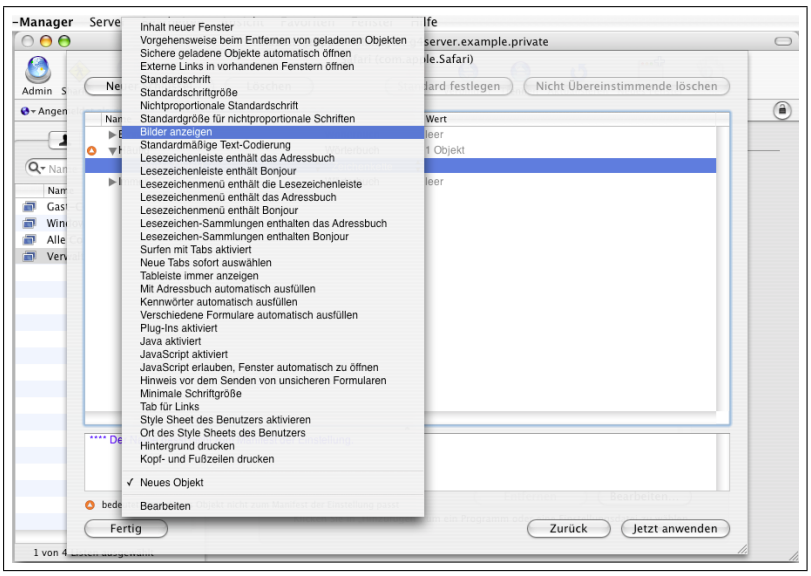

Abbildung 6.20: Besitzt ein Programm ein Einstellungsmanifest, so kann der Arbeitsgruppen-Manager alle Werte, die für verwaltete Einstellungen von Interesse sein könnten, auflisten. Es ist nicht mehr nötig, die Bedeutung der „rohen" plist-Schlüsselworte zu kennen.

Finder angezeigt wird. Man bezeichnet dies als *Verwaltete Netzwerkansicht*. Erinnern Sie sich hierzu an Kapitel 6.2 des Hauptbuchs. Im Normalbetrieb enthält der Netzwerkordner des Finders die folgenden Informationen:

- den Unterordner *Servers*, der vollautomatische Mounts zu definierten Dateiservern, nach Servern gruppiert, enthält. Auch der lokale Rechner selber ist als sein eigener Server aufgelistet.
- netzweit definierte Automounts mit vorbestimmten Namen. Falls vorhanden

  `/Network/Applications`

  für netzweit installierte Programme und

  `/Network/Library`

  für netzweit definierte andere Ressourcen, beispielsweise Schriftdateien.
- über Dienstentdeckungsverfahren (Service Recovery) erkannte Server, Netzdienste und Windows-NT-Domänen im lokalen Teilnetz.

Indem Sie weitere Vorgaben für den Netzwerkordner machen, können Sie in Tiger nun selbst virtuelle Unterordner für den Netzwerkordner erstellen und bestimmte

Vorgaben für die Anzeige von Netzressourcen definieren. Gliederungsmöglichkeiten des Netzwerkordners können hilfreich sein, um den Netzbenutzern die Präsentation der Netzumgebung so übersichtlich wie möglich zu gestalten.

Das Verwalten des Netzwerkordners ist für sehr große, sehr heterogen zersplitterte Netze gedacht. Dort kommt man oft nicht umhin, dass Benutzer auch einmal manuell eine Verbindung zu einem bestimmten Server im Netz herstellen müssen. In einem kleinen Netz ist das weniger sinnvoll. Hier bleibt es natürlich wesentlich komfortabler, mit Automounts zu arbeiten, so dass Netzwerkordner bereits an der „richtigen" Stelle im Dateisystem erscheinen, ohne dass sich die Benutzer um Server und Details des Netzes kümmern müssen.

Auf den ersten Blick scheinen die Einstellungen für den Netzwerkordner sich wie verwaltete Einstellungen zu verhalten. Im Detail sieht dies jedoch anders aus: Die Einstellungen werden nicht spezifischen Benutzern oder Gruppen zugeordnet. Sie werden deshalb nicht wie üblich an Konten gebunden. Stattdessen wird diese Art von Einstellung bestimmten Computern oder einem IP-Teilnetz zugewiesen. Aus diesem Grund wird dafür im Arbeitsgruppen-Manager ein komplett neuer Aufgabenbereich eingeführt. Es handelt sich um das neue Symbol NETZWERK in der Symbolleiste.

Doch Vorsicht: Die Einstellungen für den Netzwerkordner nutzen Computereinträge. Hierbei handelt es sich um die gleichen Einträge, die auch in den Computerlisten-Accounts verwendet werden, um einen Computer zu beschreiben. Von daher besteht schon eine Wechselwirkung zwischen dem Aufgabenbereich ACCOUNTS und dem Aufgabenbereich NETZWERK, die auf den ersten Blick nicht ganz einfach zu verstehen ist.

Sie sollten im Hinterkopf behalten, dass es in Mac OS X *Computerkonten* gibt, die aber aus Sicht des Arbeitsgruppen-Managers nur indirekt, entweder als Mitglied einer Computerliste (siehe Abschnitte 5.2.1 und 5.7.5 des Hauptbuchs) oder als Eintrag für verwaltete Netzwerkansichten angelegt werden können. Die überarbeitete Eingabemaske in Tiger zum Anlegen der Computerkonten zeigt Abbildung 6.21. Die obere Hälfte mit den Feldern NAME, COMPUTERLISTE, ETHERNET-ID spiegelt die Rolle des Eintrags bei seiner Verwendung in einem Computerlisten-Account wider, die untere Hälfte mit den Punkten NETZWERKANSICHT und URLS dient der Verwendung innerhalb einer verwalteten Netzwerkansicht. Über das Aufdeckungsdreieck WEITERE OPTIONEN... gibt es zudem noch einen dritten Bereich, nämlich die Möglichkeit, optional Kommentare und Schlüsselworte eingeben zu können.

Bevor wir uns genauer um die Einstellmöglichkeiten für verwaltete Netzwerkansichten kümmern, müssen ein paar Details zum technischen Hintergrund und den von Apple verwendeten Begriffen geklärt werden.

Abbildung 6.21: Zum Anlegen eines Computerkontos wird in Tiger ein neues Dialogfenster verwendet. Es deutet die beiden Verwendungsmöglichkeiten eines Computereintrags an, nämlich entweder als Mitglied in einem Computerlistenkonto oder als Teil einer Netzwerkansicht.

6.9.2 Aufbau von verwalteten Netzwerkansichten

Eine *Netzwerkansicht* kann aus einer beliebigen Zusammenstellung der folgenden Komponenten zusammengesetzt sein:

- einem *Computer*: ein Eintrag, der einen Computer symbolisiert, der im Netzwerk Dienste anbietet. Hierzu werden Computer-Accounts verwendet.
- einer *dynamischen Liste*: eine Gruppe von Computern, die über Dienstentdeckungsverfahren (Service Recovery) im Netzwerk vorgefunden werden, wobei diese Liste jeweils aktuell von den Client-Computern anhand bestimmter vorgegebener Kriterien erstellt wird.
- einer *Netzwerkumgebung*: ein Eintrag, der die anderen Eintragstypen in einer Gruppe zusammenfasst. Hierdurch wird im Netzwerkordner ein Unterordner erstellt. Dieser Unterordner kann dann wiederum Computer, dynamische Listen und Netzwerkumgebungen enthalten.

Neben diesen drei Komponenten, aus denen sich eine Netzwerkansicht zusammensetzt, unterscheidet Apple drei Arten von Ansichten, die entscheiden, auf welchen Computern im Netz letztendlich welche Ansichtseinstellungen wirksam werden:

- **benannte Ansicht**: Eine *benannte Ansicht* ist die speziellste Form einer Netzwerkansicht. Wie der Begriff schon andeutet, muss sie mit einem Namen versehen werden. Der Name ist mit einer bestimmten Gruppe von Computern des Netzwerks verknüpft, für die die jeweiligen Ansichtseinstellungen gültig werden sollen. Die Gruppe der Computer wird entweder über deren MAC-Adresse, über deren IP-Adressen, über deren Zugehörigkeit zu einem IP-Teilnetz oder über Computerkonten bestimmt.
- **Standardansicht:** Die *Standardansicht* kann nicht selbst benannt werden, sondern trägt den von Apple vorgegebenen Namen *Standard*. Sie wird automatisch für alle Computer aktiv, die sich nicht schon innerhalb einer benannten Ansicht befinden und die einen Verzeichnisdienstsuchpfad verwenden, in dem sich der Open Directory-Server befindet, auf dem diese Ansicht definiert ist.
- **Öffentliche Ansicht:** Eine *Öffentliche Ansicht* ist die lockerste Form der Bindung, die zwischen der Definition der Ansicht und einem Client-Computer bestehen kann. Ist ein Computer nicht bereits an eine benannte Ansicht gebunden und ist auch keine Standardansicht in seinem Verzeichnisdienstsuchpfad vorhanden, so fragt er im Netz, ob nicht *irgendein* Open Directory Server Ansichtseinstellungen bereitstellt, die er verwenden könnte. In diesem Fall wird eine Ansicht mit dem Namen *Öffentlich* aktiv.

6.9.3 Erstellen einer verwalteten Netzwerkansicht

Im folgenden Beispiel möchten wir kurz zeigen, wie eine verwaltete Netzwerkansicht eingerichtet und verwendet werden kann.

1. Starten Sie den Arbeitsgruppen-Manager und melden Sie sich mit einem geeigneten Kennwort bei einem Verzeichnisdienstserver an, für dessen Netzumgebung eine verwaltete Netzwerkansicht definiert werden soll.

2. Es erscheint ein Dialogfenster, mit dem Sie den Typ der Netzwerkansicht auswählen müssen. Entscheiden Sie sich für einen der Typen *benannt*, *Standard* oder *öffentlich* und drücken Sie die Schaltfläche ERSTELLEN.

3. In der Übersicht auf der linken Seite wird der Name der neuen Ansicht hinzugefügt, ebenso wird der neue Name auf der rechten Seite in einem Eingabefeld aufgeführt, so dass Sie ihn ändern können. Handelt es sich um eine benannte Ansicht, so müssen Sie den Namen nach bestimmten Regeln vergeben, denn der Name bestimmt, für welche Gruppe von Computern die Ansichtseinstellungen gültig werden. Folgende Namen sind möglich:

   - Sie geben die MAC-Adresse des betreffenden Computers an, für den die Einstellung gelten soll.
   - Sie geben die IP-Adresse des Computers an, für den die Einstellung gelten soll.
   - Sie geben eine Teilnetzadresse in CIDR-Schreibweise an, um damit eine ganze Gruppe von Computern auszuwählen. Das Teilnetz 192.168.1.0 mit der Maske 255.255.255.0 wird in CIDR-Schreibweise zum Beispiel als *192.168.1.0/8* geschrieben. Nähere Hinweise finden Sie unter dem Stichwort *CIDR-Schreibweise* im Hauptbuch.
   - Sie geben eine frei gewählten Namen an, und müssen diesen Namen anschließend noch in einem zweiten Schritt an ein Computerkonto knüpfen. Dies wird weiter unten beschrieben.

   Das Ankreuzfeld AKTIVIERT ermöglicht es, eine eingerichtete Ansicht kurzfristig aus- und einzuschalten. Sie können somit auch „ruhende" Einstellungen in Reserve halten.

4. Betätigen Sie die Schaltfläche mit dem Plus-Zeichen unterhalb der Tabelle. Es erscheint ein Menü, mit dem Sie eine neue Netzwerkumgebung, einen Computer oder eine dynamische Liste hinzufügen können. Durch Wiederholung dieses Schritts stellen Sie nach und nach die Netzwerkansicht zusammen, wobei sich die einzelnen Einträge in der Tabelle der Rubrik LAYOUT sammeln.

Fügen Sie eine neue Netzwerkumgebung hinzu, so erscheint ein entsprechendes Ordnersymbol in der Tabelle. Sie müssen nur noch einen neuen Namen für den Ordner angeben. Dies entspricht der Vorgehensweise wenn Sie über den Finder einen neuen Ordner im Dateisystem anlegen würden. Sie können Einträge übrigens auch mit der Maus in Ordner verschieben, ganz so wie Sie es auch im Finder machen würden.

Legen Sie einen Eintrag vom Typ *Computer* an, so erscheint das Dialogfenster zum Eingeben von Computerkonten, das wir oben bereits erwähnt haben. Bitte beachten Sie, dass Sie kein neues Computerkonto an dieser Stelle anlegen müssen, wenn Sie den betreffenden Computer bereits in einem Computerlisten-Account

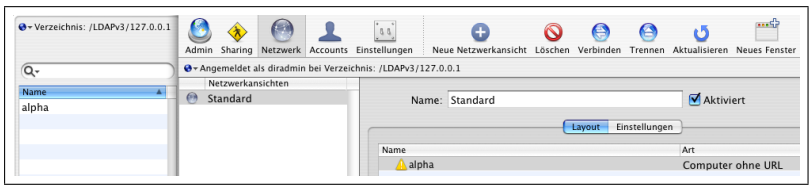

Abbildung 6.22: Wird ein bereits bestehendes Computerkonto als Computereintrag in eine verwaltete Netzwerkansicht übernommen, so ist dies durch Einblendung des Schubfachs und Ziehen mit der Maus möglich. Der Arbeitsgruppen-Manager warnt, wenn ein Kontoeintrag noch zu unvollständig ist, um ihn für die verwaltete Ansicht einsetzen zu können.

aufgeführt haben. In diesem Fall ist es einfacher, bzw. zum korrekten Aufbau Ihrer Computerlisten vielleicht sogar erforderlich, wenn Sie sich an dieser Stelle auf ein bereits bestehendes Computerkonto beziehen. (Wenn Sie ein neues Computerkonto über den Funktionsbereich NETZWERK anlegen und das Klappmenü COMPUTERLISTE unberührt lassen, erscheint der Computer im Funktionsbereich ACCOUNTS automatisch in der Computerliste *Alle Computer*.) Wählen Sie bei einem bereits bestehenden Computerkonto bei der Plus-Schaltfläche den Menüpunkt COMPUTER EINBLENDEN. . . . Es erscheint ein Schubfach mit einer Liste aller Computerkonten. Durch Ziehen mit der Maus können Sie Einträge direkt in die Layout-Tabelle übertragen. Mit einem Achtung-Symbol warnt Sie der Arbeitsgruppen-Manager, falls im Computerkonto zu wenig Felder ausgefüllt sind, um den Computer als Netzwerkansichtseintrag verwenden zu können (Abbildung 6.22).

Einen Computereintrag in eine verwaltete Netzwerkansicht einzufügen, heißt, dass Sie den betreffenden Computer in den Netzwerkordner einblenden möchten und dass beim späteren Anklicken im Finder einer oder mehrere Dienste abrufbar sein sollen. Aus diesem Grund muss jeder Eintrag mit mindestens einer Dienstadresse in Form einer URL versehen werden. Sie tragen diese Adressen in die Tabelle URL des Dialogfensters für das Computerkonto ein und bestätigen außerdem über das Klappmenü NETZWERKANSICHT für welche Ansicht das Computerkonto gültig werden soll.

Beispiel: Sie haben im Netz einen Fileserver für die Protokolle AFP und CIFS/SMB, den Sie unter dem Begriff *Fileserver* standardmäßig in den Netzwerkordner einblenden möchten. Die MAC-Addresse für die primäre Ethernet-Schnittstelle des Servercomputers lautet *00:0d:93:4e:56:fd*, im Netzwerk besitzt er den DNS-Namen *g4server.example.private*. Nach Auswahl der gewünschten Netzwerkansicht betätigen Sie die Plus-Taste unterhalb der Layout-Tabelle, um den Punkt NEUER COMPUTER. . . aufzurufen. Sie geben in das Feld NAME den Wert *Fileserver* ein und tragen in das Feld ETHERNET-ID den Inhalt *00:0d:93:4e:56:fd* ein. Neben der Tabelle URLS betätigen Sie die Plus-Schaltfläche, um die Zeile

```
afp://g4server.example.private
```

einzugeben. Sie wiederholen den letzten Schritt, um ebenso die Adresse

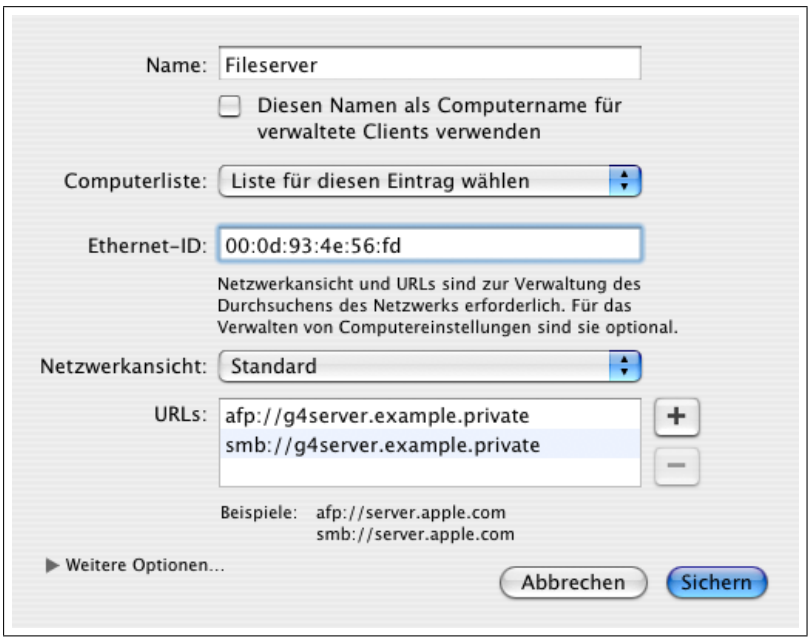

Abbildung 6.23: Einrichten eines neuen Computereintrags für eine verwaltete Netzwerkansicht

```
smb://g4server.example.private
```

einzutragen. Danach betätigen Sie die Schaltfläche SICHERN. Siehe hierzu auch Abbildung 6.23. Wenn Sie auch den Knopf SICHERN des Aufgabenbereichs NETZWERK betätigen, wird der Eintrag wirksam.

Beachten Sie, dass in diesem Beispiel ein neues Computerkonto angelegt wurde, für das noch kein Eintrag in einem Computerlistenkonto (oder in einer anderen verwalteten Netzwerkansicht) bestanden hat. Wir haben das Klappmenü COMPUTERLISTE nicht berührt, sondern es auf dem Standardwert LISTE FÜR DIESEN EINTRAG WÄHLEN belassen. Das neue Konto wurde hierdurch der vordefinierten Computerkontenliste *Alle Computer* zugeordnet, was Sie im Bereich ACCOUNTS überprüfen können.

Eine alternative Methode, einen neuen Computereintrag zu erzeugen, besteht darin, in diesem Moment auf dem Computer, auf dem der Arbeitsgruppen-Manager gerade läuft, eine Dienstentdeckung anzustoßen. Sie können dann einen der gefundenen Einträge als Computereintrag in die Tabelle übernehmen. Drücken Sie hierzu die Taste mit den drei Punkten unterhalb der Layout-Tabelle. Im erscheinenden Dialogfenster müssen Sie den etwas verwirrend beschrifteten Knopf VERBINDEN drücken, um einen ausgewählten Eintrag zu übernehmen.

Der dritte Kategorie von Einträgen betrifft wie erwähnt die dynamischen Listen. Wählen Sie hierzu über das Pluszeichen unterhalb der Tabelle den Punkt DYNAMI-

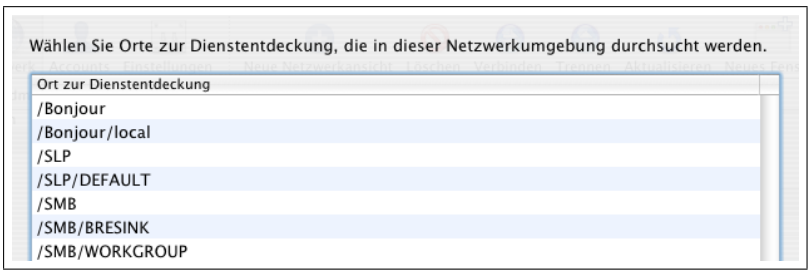

Abbildung 6.24: Fügen Sie einen Eintrag des Typs *Dynamische Liste* einer verwalteten Netzwerkansicht hinzu, müssen Sie alle Dienstentdeckungsbereiche, die verwendet werden sollen, auswählen.

SCHE LISTE HINZUFÜGEN... aus. Es erscheint ein Dialogfenster, das alle Dienstentdeckungsdomänen, die im lokalen Netz gefunden werden, auflistet. Die Bereiche werden in Form von Verzeichnisdienstpfaden (siehe Abschnitte 6.2.1 und 7.2.5 des Hauptbuchs) angegeben (Abbildung 6.24). Sie müssen einen oder mehrere Suchbereiche für die Dienstentdeckung auswählen und dann den Knopf HINZUFÜGEN drücken.

Einträge in der Tabelle können mit dem Minus-Symbol gelöscht und mit dem Stift-Symbol verändert werden. Es sei darauf hingewiesen, dass die komplexen Möglichkeiten der Wiederverwendung von Computerkonten teilweise auch den Arbeitsgruppen-Manager selbst überfordern. In einigen Versionen von Mac OS X Tiger erhalten Sie in vielen Fällen Meldungen wie in Abbildung 6.26. In einem solchen Fall bleibt Ihnen oft nur noch die Möglichkeit, eine verwaltete Netzwerkansicht komplett zu löschen, oder sie „roh“ in der LDAP-Datenbank zu bearbeiten.

6.9.4 Zuweisung verwalteter Netzwerkeinstellungen an Klienten

Wir hatten bereits erwähnt, dass benannte Netzwerkansichten, die in ihrem Namen weder ein Teilnetz in CIDR-Schreibweise, noch eine IP-Adresse, noch eine MAC-Adresse aufführen, zunächst keinem Client-Computer zugewiesen werden. Sie müssen in dem Fall die Computer einzeln aufführen, die in ihrem Netzwerordner die entsprechende Netzwerkansicht einblenden sollen. Hierzu dient die Karteikarte EINSTELLUNGEN.

1. Wählen Sie in der linken Tabelle NETZWERKANSICHTEN einen Eintrag aus, der so benannt ist, dass Client-Computer ihm nicht automatisch zugeordnet werden können.
2. Wählen Sie in der rechten Hälfte des Fensters die Karteikarte EINSTELLUNGEN aus.
3. Betätigen Sie die Plus-Schaltfläche rechts neben der Tabelle CLIENTS. Es er-

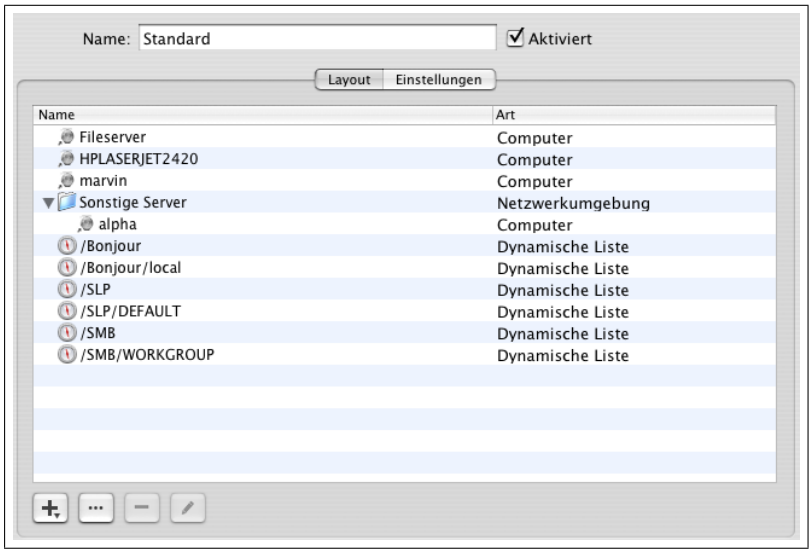

Abbildung 6.25: Ein Beispiel für eine fertig definierte verwaltete Netzwerkansicht

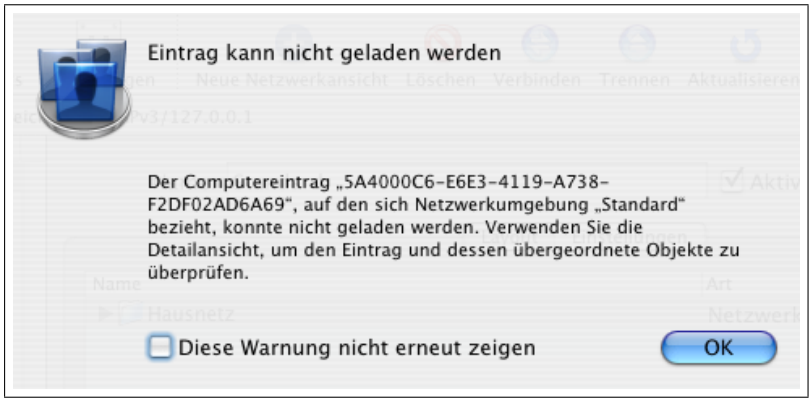
Eintrag kann nicht geladen werden
Der Computereintrag „5A4000C6-E6E3-4119-A738-F2DF02AD6A69“, auf den sich Netzwerkumgebung „Standard“ bezieht, konnte nicht geladen werden. Verwenden Sie die Detailansicht, um den Eintrag und dessen übergeordnete Objekte zu überprüfen.
Diese Warnung nicht erneut zeigen
OK

Abbildung 6.26: Die vielen Querbeziehungen zwischen Computerlisten, Computerkonten und verwalteten Netzwerkansichten scheinen oft auch den Arbeitsgruppen-Manager zu überfordern. Ein beschädigter Eintrag muss gelöscht oder von Hand repariert werden.

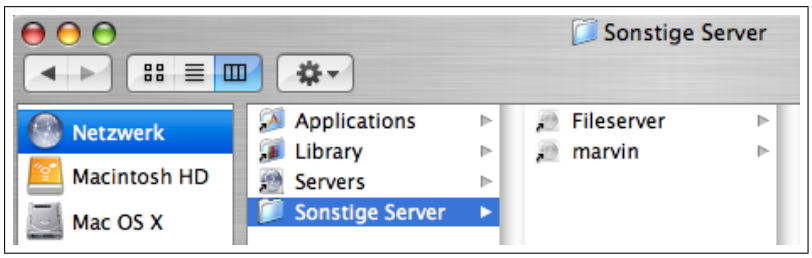

Abbildung 6.27: Das Ergebnis der ganzen Bemühungen: Im Netzwerkordner der Client-Computer erscheinen selbst definierte Einträge

scheint ein Menü, mit dem Sie entweder ein neues Computerkonto erstellen können oder das Schubfach öffnen, um bereits vorhandene Computerkonten in die Tabelle zu ziehen.

Unterhalb der Tabelle können Sie noch zwei wichtige Einstellungen für die ausgewählte Netzwerkansicht vornehmen. Mit dem Punkt CLIENTS SUCHEN NACH ÄNDERUNGEN ALLE können Sie einen Zeitraum einstellen, nach dem alle Client-Computer, die diese verwaltete Netzwerkansicht verwenden, prüfen, ob sich an den Ansichtseinstellungen etwas geändert hat. Hier ist zu raten, eine recht kurze Zeit einzustellen, während Sie mit verwalteten Netzwerkeinstellungen zum ersten Mal experimentieren. Später sollten Sie jedoch für den Normalbetrieb ein größeres Zeitintervall verwenden. Apple schlägt 10 Stunden vor.

Die Option FINDER DES CLIENT WIRD gibt an, wie im Detail mit der verwalteten Ansicht verfahren werden soll. In der Einstellung ZUR NETZWERKANSICHT HINZUFÜGEN wird der Finder auf den betroffenen Client-Computern die durch die verwalteten Einstellungen gegebenen Punkt zu seinen „normalen“ Objekten im Netzwerkordner hinzufügen. Wird jedoch die Einstellung NETZWERKANSICHT ERSETZEN eingestellt, so wird – bis auf symbolische Links und Mount Points – der gesamte Inhalt des Netzwerkordners durch die Objekte der verwalteten Netzwerkansicht ersetzt.

Kapitel 7

Die Dateiserverfunktionen

7.1 Maximale Pfadlängen bei Verwendung von Automounts für Privatordner

In der Vergangenheit hat Apple mehrmals Änderungen bezüglich der Strategie durchgeführt, wie der Automounter von Mac OS X die Pfade für die symbolischen Links auf Client-Seite zusammengesetzt hat (siehe hierzu Abschnitt 6.3.1 im Hauptbuch). Diese Änderungen haben während der Lebenszeit von Panther zu kritischen Problemen geführt. In manchen Systeminstallationen wurden Automount-Einträge für die privaten Home-Ordner der Benutzer ungültig, weil eine bestimmte Länge der Ordnerpfade überschritten wurde. Apple hat sich daher veranlasst gesehen, bestimmte Vorschriften über die maximale Länge der Pfadangaben für Privatordner zu machen. Die maximale Länge bezieht sich auf die Anzahl der Zeichen, die zur Speicherung des BSD-Dateipfades zum Zugriff auf einen privaten Ordner auf einem Client-Computer verwendet wird.

Beispiel: Auf unserem Server *g4server.example.private* haben wir einen über AFP geshareten Ordner für die privaten Ordner aller Netzwerkbenutzer eingerichtet, der auf einem zweiten Volume unter dem Server-Pfad

```
/Volumes/UserStuff/Users
```

liegt. Hierzu passend wurde im Arbeitsgruppen-Manager außerdem ein Automount-Eintrag mit der Option „PRIVAT“-ORDNER FÜR BENUTZER erstellt. Führt nun ein Netzwerk-Client unter Mac OS X Tiger den diesbezüglichen Automount durch, so legt der Automounter auf dem Klienten einen Mount-Point an, der mit dem Pfad

```
/private/Network/Servers/g4server.example.private/Volumes/UserStuff/Users
```

zu erreichen ist. In unserem Beispiel beträgt die Länge dieses Pfades 73 Zeichen.

Betriebssystemversion	Maximale Länge des Mount-Pfads
Mac OS X 10.2 bis 10.2.8	65 Zeichen
Mac OS X 10.3 bis 10.3.4	51 Zeichen
Mac OS X 10.3.5 bis 10.3.9	65 Zeichen
Mac OS X 10.4 bis 10.4.2	73 Zeichen

Tabelle 7.1: Maximal erlaubte Längen für Pfade zum Automount von Privatordnern auf Client-Computern

Aufgrund von verschiedenen Beschränkungen der am Automount-Prozess beteiligten Programme garantiert Apple nur dann, dass der Automount unter allen denkbaren Umständen funktioniert, wenn die Längen aus Tabelle 7.1 nicht überschritten werden. Die maximalen Längen hängen von den Betriebssystemversionen ab, die auf den Clients eingesetzt werden. Es spielt keine Rolle, ob AFP oder NFS als Protokoll genutzt wird.

7.2 Einschränkungen des NFS-Servers

Wie in Abschnitt 6.6.3 des Hauptbuchs erläutert, gelten für das Freigeben von Ordnern über NFS spezielle Regeln, die beachtet werden müssen. Diese Regeln gelten grundsätzlich für alle NFS-Server, egal von welchem Hersteller sie stammen und unter welchem Betriebssystem sie laufen. Für Mac OS X hat Apple inzwischen eine weitere, spezielle Einschränkung dokumentiert, die beachtet werden sollte.

Wenn Sie einen NFS-Export so anlegen, dass die zugreifenden Client-Rechner nicht überprüft werden – in Apples Terminologie also einen Export an „World" vornehmen (siehe Abbildung 7.1) – dann akzeptiert Mac OS X dies nur auf einem einzigen Volume. Ist Ihr Server-Computer zum Beispiel mit drei Partitionen ausgestattet oder besitzt drei Festplatten und Sie geben eines dieser Volumes per NFS mit dem Klienten-Zugriffsrecht WORLD frei, so dürfen Sie keinen anderen Volumes ebenfalls über NFS an WORLD exportieren.

Tun Sie dies trotzdem, so ignoriert Mac OS X die zusätzlichen Freigaben völlig. Nur der Exporteintrag, der in der internen Datenbank als letzter definiert wurde, funktioniert. Dies ist insbesondere für den Fall wichtig, wenn Sie mit der NetBoot-Funktion arbeiten. Die Betriebssystem-Images werden in der Regel per NFS freigegeben und Mac OS X muss in diesem Fall einen World-Export verwenden, was auch automatisch so konfiguriert wird. Beachten Sie also diese Einschränkungen, wenn Sie den NetBoot-Ordner *NetBootSPx* auf einem Volume haben einrichten lassen.

Abbildung 7.1: Ein Volume kann per NFS an beliebige Client-Computer freigegeben werden, was Apple als „World“-Export bezeichnet. Es ist zu vermeiden, auf einem Server mehr als einen Export mit dieser Einstellung einzurichten.

7.3 Über AFP auf NFS: Resharing

In früheren Versionen war es nötig, manuelle Änderungen an der NetInfo-Datenbank vorzunehmen, um ein *AFP-zu-NFS-Resharing* einzurichten. Wie in Abschnitt 6.7 des Hauptbuchs erläutert, handelt es sich hierbei um die Technik, Mac OS X Server ein NFS-Volume eines Unix-Rechners mounten zu lassen und dieses per AFP an Macintosh-Klienten wieder neu freizugeben. Der Server kann somit als Vermittler zwischen NFS-Servern und AppleShare-Klienten dienen. Ab Mac OS X Tiger ist die Einrichtung dieser Funktion über die grafische Oberfläche möglich. Auch ist es nicht mehr notwendig, einen leeren Ordner für den NFS-Mount-Point auf dem Server anzulegen.

1. Beachten Sie die Sicherheitshinweise aus Kapitel 6.7 des Hauptbuchs. Der NFS-Server darf Zugriffe des Benutzers *root* nicht abblocken oder auf einen anderen Benutzer abbilden.
2. Starten Sie den Arbeitsgruppen-Manager, verbinden Sie sich mit dem Server, der als AFP-Server dient.
3. Wählen Sie in der Symbolleiste den Punkt SHARING aus.
4. Wechseln Sie in der linken Hälfte des Fensters auf den Punkt ALLE.
5. Klicken Sie auf die zweite Schaltfläche unterhalb der Tabelle (Abbildung 7.2). Diese Taste dient zum Arbeiten mit NFS-Mounts.

6. Geben Sie die Adresse des NFS-Exports als URL ein. Im Hauptbuch wurde auf dem NFS-Beispielserver *linux* eine Freigabe */exports/home* verwendet. Die Adresse würde in URL-Form

   ```
   nfs://linux/exports/home
   ```

   lauten.

7. Mac OS X richtet einen Ordner *nfs_reshares* ein und blendet dort das NFS-Volume ein. Als Name wird die letzte Pfadkomponente der Exportdefinition verwendet. In unserem Beispiel würde Sie den Mount also unter

   ```
   /nfs_reshares/home
   ```

   finden. Das Netzwerk-Volume wird in der am weitesten links stehenden Spalte der Tabelle ALLE angezeigt.

8. Wählen Sie diesen neuen Eintrag in der Tabelle ALLE aus und richten Sie eine Freigabe über das AFP-Protokoll ein, wie Sie es gewohnt sind.

In den ersten Versionen von Tiger zeigt der Finder fälschlicherweise ein Auswurf-Symbol *(Eject)* für das NFS-Netzvolume an, obwohl es sich um einen statischen Automount handelt. Sie sollten es vermeiden, das Auswurfsymbol anzuklicken, da der Finder damit nicht richtig zurechtkommt.

Leider unterstützt diese Vorgehensweise nur NFS-Mounts, die mit Standardeinstellungen durchgeführt werden können. Da Apple nur die Eingabe einer URL erlaubt, können keine Optionen zur Verbindungsherstellung angegeben werden. Viele NFS-Server benötigen aber zum Beispiel die Sicherheitsoption `-P`, damit der Server den Zugriff von Mac OS X akzeptiert. Sie müssen in diesem Fall doch wieder – zumindest teilweise – auf das manuelle Ändern der NetInfo-Datenbank zurückgreifen. Folgen Sie hierzu der Anleitung im Hauptbuch ab Schritt (11), um bei dem erstellen Mount-Eintrag eine Eigenschaft *opts* zu definieren, und sie mit Optionen zu versehen.

7.4 Der CIFS/SMB-Server

7.4.1 Sicherungs-Domänen-Controller

Im Server Admin-Programm können Sie auf der Karteikarte ALLGEMEIN nun den Einsatz des Windows-Dienstes als *Sicherungs-Domänen-Controller* auswählen. Diese Funktion, die auch *BDC* oder *Backup Domain Controller* genannt wird, ist die in der Microsoft-Welt übliche Technik, die *Verzeichnisreplikation* zu realisieren.

Sollte der Server ausfallen, der die Windows-Verzeichnisdienste beherbergt, würde dies sofort den Ausfall aller Windows-Klienten im Netz bedeuten, da diese nicht

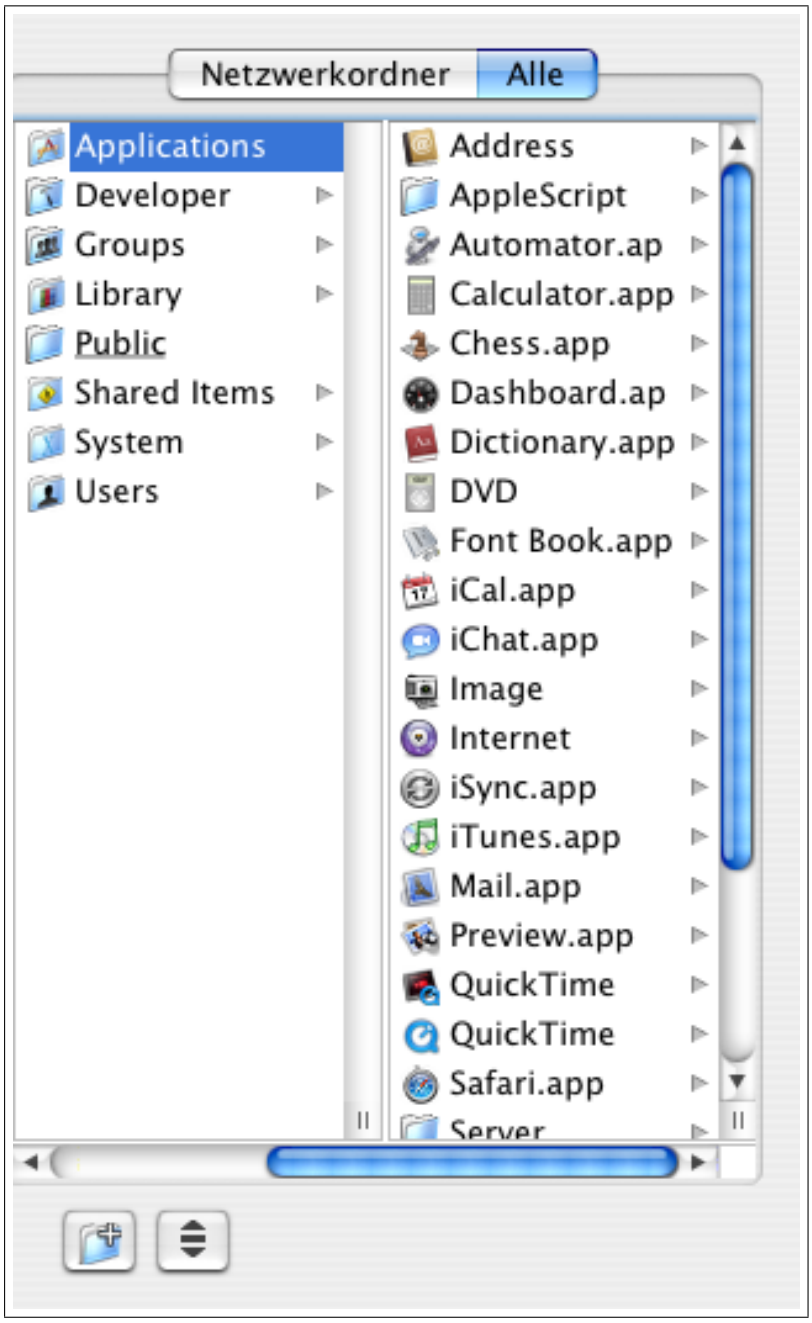

Abbildung 7.2: Der Arbeitsgruppen-Manager ist nun selbständig in der Lage, einen statischen NFS-Automount einzurichten, der per AFP wieder freigegeben werden kann. Hierzu befindet sich eine neue Schaltfläche unterhalb der Tabelle im Bereich Sharing. Über diese Taste lässt sich ein Eintrag übrigens auch wieder entfernen.

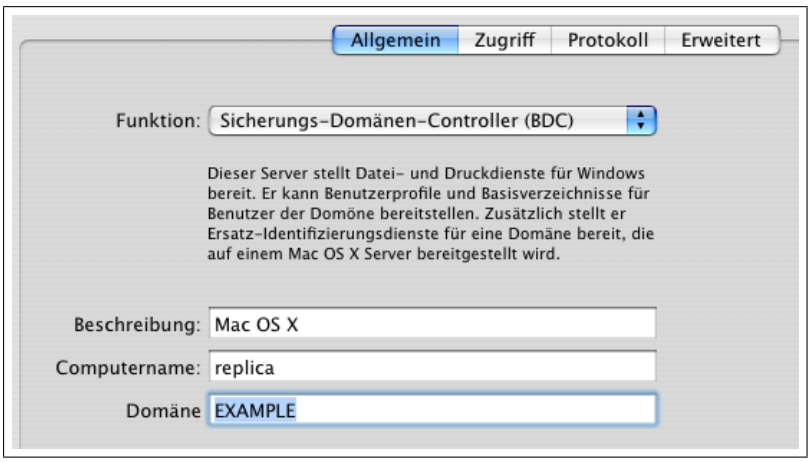

Abbildung 7.3: Arbeitet ein Server bereits als Open Directory Replik eines anderen Servers, so kann er durch simples Wechseln der Einstellung FUNKTION der Windows-Dienste auch als Sicherungs-Domänen-Controller arbeiten.

mehr an ihre Verwaltungs- und Authentifizierungsdaten kommen. Um dies zu vermeiden, können ein oder mehrere Sicherungs-Domänen-Controller eingerichtet werden, die die Daten des *primären Domänen-Controllers (PDC)* spiegeln und diesen im Notfall vollständig ersetzen können. Gleichzeitig wird die Leistung verbessert: Sollte der PDC kurzfristig überlastet oder durch hohen Netzverkehr schlecht erreichbar sein, können sich die Client-Computer automatisch mit einem Sicherungs-Domänen-Controller verbinden, der schneller reagiert.

Ein BDC arbeitet also als Replik eines PDC, genau wie eine *Open Directory Replik* als Sicherung eines Open Directory Masters arbeitet. Konsequenterweise hat Apple diese beiden Parallelen miteinander verknüpft: Sie können nur dann einen Mac OS X Server als BDC einsetzen, wenn dieser auch gleichzeitig als Open Directory Replik konfiguriert ist. Gedacht ist es so, dass Sie im Netz einen Hauptserver als Open Directory Master und PDC einrichten, der sowohl von Macintosh-, Windows- und Unix-Klienten benutzt werden kann. Danach sichern Sie beide Verzeichnisdienste über die Aufstellung eines oder mehrerer Replikationsserver gegen Ausfälle ab. Jeder Replikationsserver arbeitet dann als Open Directory Replik und Windows-BDC.

7.4.2 Neue Identifizierungsmethoden

Mac OS X Server unterstützt neue Identifizierungsverfahren zum Anmelden von Benutzern an den Windows-Diensten. In Server Admin können Sie für den Dienst WINDOWS unter EINSTELLUNGEN | ZUGRIFF | IDENTIFIZIERUNG das neue Ankreuzfeld NTLMv2 & KERBEROS finden (Abbildung 7.4). Hierbei handelt es ich um Identifizierungsverfahren, die zum Einsatz kommen, wenn der Server Mitglied einer Windows

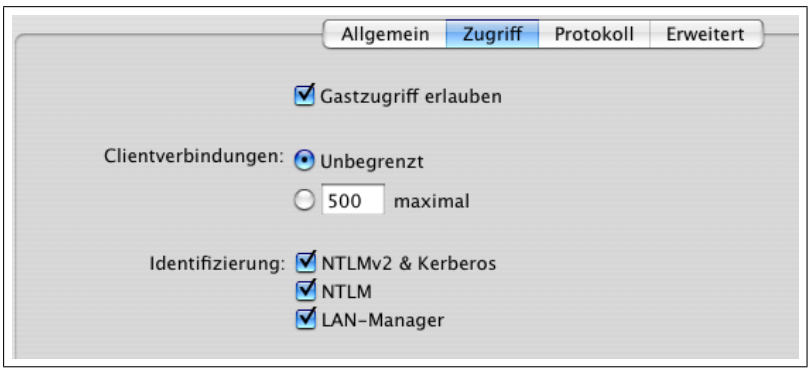

Abbildung 7.4: NTLMv2 & Kerberos sind aktuelle Identifizierungsverfahren der Windows-Welt, die ab Tiger auch für Mac OS X Server zur Verfügung stehen.

Active Directory-Domäne wird, beziehungsweise im Zusammenhang mit Windows 2000 Server und Windows Server 2003 eingesetzt wird. Sie können damit das aktuelle Kennwortprüfungsverfahren von Windows und die Gesamt-Authentifizierung (Single Sign-On) auch für CIFS/SMB-Dienste von Mac OS X verwenden.

7.5 Probleme in gemischten Netzen

7.5.1 Kompatibilitätsprobleme des NFS-Automounters

Die grundlegenden Probleme, die in Abschnitt 6.10.4 des Hauptbuchs beschrieben werden, bestehen auch weiterhin. Eine der denkbaren Lösungsmöglichkeiten steht in Mac OS X ab Version 10.4 jedoch nicht mehr zur Verfügung: Der alternative Berkeley-Automounter *AMD* wird in Tiger nicht mehr mitgeliefert und auch das Startskript, das über die */etc/hostconfig* aktiviert werden konnte, ist nicht mehr enthalten.

Falls Sie experimentierfreudig sind, können Sie sich eine Darwin-Version von AMD aus dem Quellcode erstellen und selbst installieren. Dokumentation und Quellcode sind über die Website

```
http://www.am-utils.org/
```

erhältlich. Es sei allerdings nochmals darauf hingewiesen, dass zu Redaktionsschluss der NIS-Klient in Tiger unbrauchbar war, so dass die Installation eines eigenen Automounters für NFS/NIS-Netze nicht unbedingt zu einer funktionierenden Lösung führt.

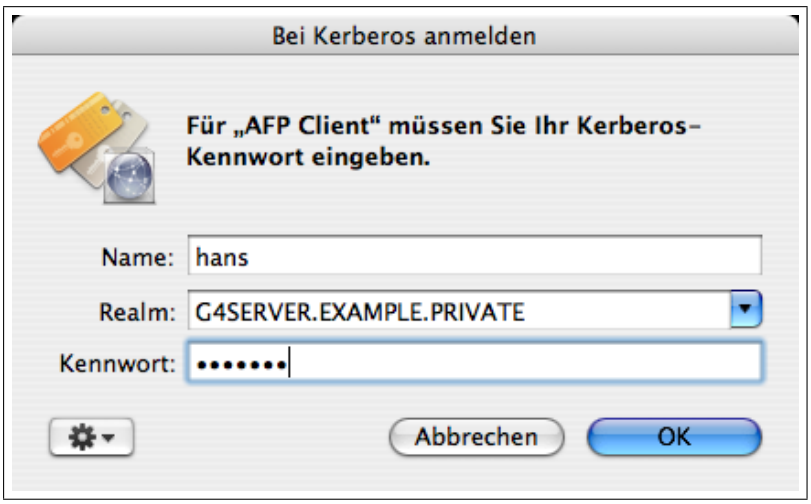

Abbildung 7.5: Das Dialogfenster für die Anmeldung über Kerberos wurde in Tiger stark überarbeitet.

7.6 Unerwünschten Kerberos-Einsatz verhindern

Die Vorgehensweise, um den Einsatz von Kerberos in den Situationen zu verhindern, in den die Gesamt-Authentifizierung nicht erwünscht ist, hat sich nicht geändert. Apple hat allerdings die Gestaltung sowohl des Kerberos-Anmeldefensters als auch des Kerberos-Wartungsprogramms stark überarbeitet. Außerdem sind die Programme nun vollständig in die deutsche Sprache übersetzt.

Abbildung 7.5 zeigt das neue Anmeldefenster. Die früheren Zusatzoptionen, die in Panther über einen Aufklapppfeil zur Verfügung standen, sind jetzt über ein Menü abrufbar, das mit der Zahnradtaste links unten geöffnet wird. Neu ist die Funktion, an dieser Stelle auch das Kerberos-Kennwort ändern zu können.

Das Wartungsprogramm für Kerberos-Tickets in Mac OS X Tiger zeigt die Abbildung 7.6. Auch hier steht über die Symbolleiste eine neue Möglichkeit zur Verfügung, das Kennwort direkt vom Benutzer ändern zu lassen.

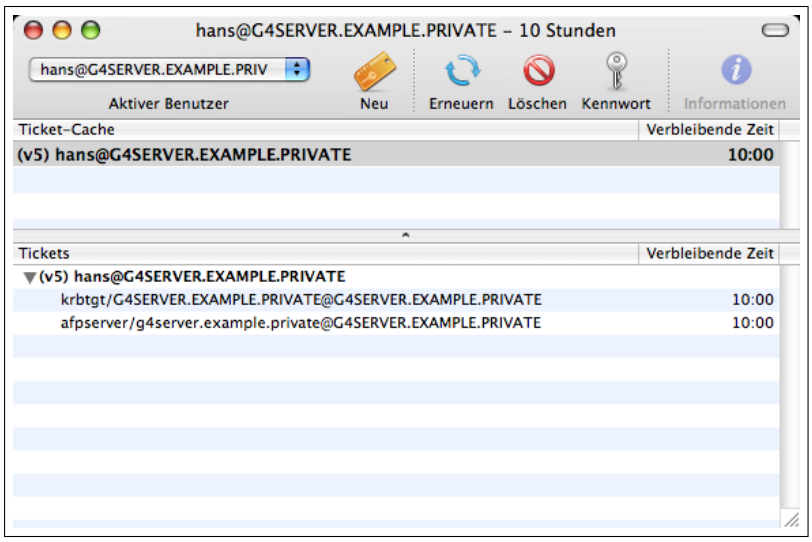

Abbildung 7.6: Ebenso hat das Programm zur Verwaltung von Kerberos-Tickets eine neue Oberfläche bekommen. Es steht jetzt auch in deutscher Sprache zur Verfügung.

Kapitel 8

Verzeichnisdienste

8.1 Unterstützte Informationskategorien

Apple hat viele Informationskategorien in den Directory Services ergänzt und ein paar Eintragstypen umbenannt. Im Wesentlichen betrifft dies die Speicherung von Daten für neue Features und die weitere Vereinheitlichung der früheren NetInfo- mit der heutigen LDAP-basierten Verzeichnisdienststrategie in Mac OS X . Tabelle 8.1 zeigt die geänderten Eintragungen. Die vollständige Tabelle ist in Abschnitt 7.2.4 des Hauptbuchs enthalten.

8.2 Quellen für Verwaltungsinformationen

Apples Version der Technik *ZeroConf* zur vollautomatischen Konfiguration und Diensterkennung in TCP/IP-Netzen heißt in Tiger nicht mehr *Rendezvous*. Aus markenrechtlichen Gründen musste diese Technologie in *Bonjour* umbenannt werden.

8.3 Das Lookup-Subsystem

Die klassische Unix-Technik zur Zuordnung von MAC-Adressen zu IP-Adressen wird in den Verzeichnisdiensten unterstützt. Der *FFAgent* des Lookup-Subsystems verwendet die übliche BSD-Konfigurationsdatei

```
/etc/ethers
```

um nach diesen Daten zu suchen.

Informationskategorie	Bezeichnung im Lookup-Subsystem	Bezeichnung in Directory Services
Zugriffsrechte auf Verzeichnisdienstdaten	–	AccessControls
Verweise auf Benutzerkonten (AFP)	–	AFPUserAliases
E-Mail-Aliasnamen von Benutzern	aliases	Aliases
Beschreibung der Verzeichnisdienstdaten	–	AppleMetaRecord
Daten für Serverkonfiguration	–	AutoServerSetup
Server für NetBoot (BootP-Protokoll)	bootp	Bootp
Zertifikatsstellen	–	CertificateAuthorities
MAC-Adressen	ethers	Ethernets
FileMaker Datenbankserver	–	FileMakerServers
Computernamen	hosts	Hosts
Serverdienste	–	HostServices
Standort von verteilten Netzdiensten	locations	Locations
Verwaltete Netzansichten	–	Neighborhoods
Domänen	–	NetDomains
Computergruppen	netgroups	NetGroups
Netzwerknamen	networks	Networks
Kennwortserver	–	PasswordServer
Personenbezogene Kontaktdaten	–	People
Druckserverdienst	–	PrintService
Benutzer eines Druckserverdienstes	–	PrintServiceUser
TCP/IP-Protokolle	protocols	Protocols
Ferne Prozeduraufrufe (SUN RPCs)	rpcs	RPC
TPC/IP-Portnummern	services	Services
AFP-Freigaben	–	SharePoints

Tabelle 8.1: Liste der geänderten Informationskategorien, die Mac OS X in Verzeichnisdiensten abfragen kann. Die Tabelle ist alphabetisch nach den Directory Service-Namen geordnet.

8.4 Das Programm Verzeichnisdienste

Das Programm *Verzeichnisdienste* wurde für Tiger leicht überarbeitet. Vor allem der früher strikt getrennte Konfigurationsvorgang in den drei Programmbereichen DIENSTE, IDENTIFIZIERUNG und KONTAKTE wurde etwas benutzerfreundlicher gestaltet: In den Dialogfenstern zur Einrichtung des LDAPv3- und des NIS-Klienten unter DIENSTE stehen nun Ankreuzfelder zur Verfügung, mit denen das Hinzufügen eines gerade neu definierten Verzeichnisknotens in die Suchpfade IDENTIFIZIERUNG und KONTAKTE sofort durchgeführt werden kann. Man erspart sich so, die Punkte IDENTIFIZIERUNG und KONTAKTE noch einmal getrennt aufrufen zu müssen (Abbildung 8.1).

Auch der Dialog beim manuellen Einrichten einer Verbindung zu einem LDAP-Server wurde vereinfacht: Nachdem die Adresse des LDAP-Servers eingegeben und die wichtigsten Verbindungsparameter über das Dialogfenster in Abbildung 8.2 eingegeben wurden, verbindet sich das Programm *Verzeichnisdienste* sofort probeweise mit dem Server, um festzustellen, um welche Art von Datenbankschema es sich handelt. Wird ein Apple Open Directory-Server erkannt, ist kein weiterer Konfigurationsschritt mehr nötig, alle nötigen Daten werden dynamisch ermittelt.

Darüber hinaus gibt es eine neue Authentifizierungsmöglichkeit bei der erstmaligen Bindung an den LDAP-Server, die wir in Kapitel 9 noch detailliert beschreiben.

8.5 Die Anbindung an NIS

Bei Redaktionsschluss war die Verwendung von Mac OS X Tiger im Zusammenhang mit NIS-Netzwerken aufgrund mehrerer kritischer Fehler nicht möglich. Es wird erwartet, dass ab Mac OS X 10.4.3 die NIS-Funktionen wieder brauchbar werden. Ist dies der Fall, ergeben sich keine größeren Änderungen im Vergleich zu Panther.

8.6 NetInfo – der klassische Verzeichnisdienst

Bezüglich NetInfo hat sich Tiger gegenüber Panther nichts geändert, so dass keine Ergänzungen oder Anmerkungen zu Kapitel 8 des Hauptbuchs notwendig sind.

Lokale BSD-Dateien (/etc) zur Identifizierung verwenden
Wenn Sie die Verwendung zur Identifizierung aktivieren, wird die Verzeichnis-Domain „/BSD/local“ zur Identifizierungs-Suchrichtlinie hinzugefügt.
Konfiguration des NIS-Servers
Domain-Name: example.nis
Server: 192.168.40.66
Aus Sicherheitsgründen Name(n) oder IP-Adresse(n) des NIS-Servers hinzufügen. Sie müsen IP-Adressen verwenden, falls DNS in Ihrem Netzwerk nicht verfügbar ist.
NIS-Domain zur Identifizierung verwenden
Wenn Sie die Verwendung zur Identifizierung aktivieren, wird die Verzeichnis-Domain „/BSD/<Domain-Name>“ zur Identifizierungs-Suchrichtlinie hinzugefügt.
Abbrechen
OK

Abbildung 8.1: Das Dialogfenster für die Einrichtung des Verzeichnisdienst-Plug-Ins für lokale BSD-Dateien und NIS kann den erstellten Verzeichnisknoten sofort in den Suchpfad für die Identifizierung von Benutzern übernehmen. Das Aufrufen des Rubrik IDENTIFIZIERUNG ist nicht mehr erforderlich.

Abbildung 8.2: Auch das LDAPv3-Plug-In kann neue Verzeichnisknoten sofort in die Suchpfade einfügen. Ist der LDAP-Server ein Mac OS X Server, so ist nur noch dieses Dialogfenster auszufüllen, der Rest wird automatisch ermittelt.

Kapitel 9

LDAP und Apple Open Directory

9.1 LDAP in Mac OS X Server nutzen

9.1.1 Überwachung und Konfiguration des LDAP-Servers

Änderung der Vorgabe für den LDAP-Suchpfad

Wenn Sie einen neuen Server-Computer einrichten, hat Apple in Tiger die Strategie für die automatische Vorgabe des LDAP-Suchpfades geändert. Nicht nur der DNS-Name der Server-Domain, sondern der voll qualifizierte DNS-Name des Servers wird als Vorgabe für den LDAP-Suchpfad vorgeschlagen. Für unseren Beispielserver

```
g4server.example.private
```

wird demzufolge bei Einrichtung eines Open Directory Masters der Distinguished Name

```
dc=g4server,dc=example,dc=private
```

als Vorschlag übernommen. Auf bereits bestehende, aktualisierte Server hat dies keinen Einfluss.

Änderungen bei der Konfiguration

Rufen Sie mit dem Server Admin-Programm die Verwaltung des Dienstes OPEN DIRECTORY auf, so sind in Tiger einige neue Protokollabfragen möglich. Neben den schon in Panther vorhandenen Aufzeichnungen über Open Directory-Aktivitäten

können Sie jetzt zusätzlich über Server Admin die folgenden Protokolle anzeigen lassen:

- **kadmin-Protokoll:** Problemmeldungen und Statusberichte, die bei der Verwaltung der Kerberos-Dienste angefallen sind.
- **kdc-Protokoll:** Tätigkeitsbericht des Kerberos-Schlüsselverteilungsdienstes
- **lookupd-Protokoll:** Fehlermeldungen des lokalen Lookup-Subsystems des Servercomputers
- **Kennwort-Server-Replizierungsprotokoll:** Tätigkeitsbericht über das regelmäßigen Kopieren der Kennwortserverdaten an Replikatserver
- **slapconfig-Protokoll:** Tätigkeitsbericht für das Ändern der Such- und Verwaltungseinstellungen für den LDAP-Server und die Replizierungsfunktionen

Ganz neu ist der Punkt ARCHIVIEREN, der in Tiger Einzug in die Verwaltung des Open Directory Systems gehalten hat. Mit diesem Punkt ist es möglich, eine Datensicherung aller Open Directory-Daten durchzuführen, um eine vollständige Kopie der Daten zu haben, die im Falle eines Notfalls wieder ins System eingespielt werden kann. Um diese Funktion nutzen zu können, muss der Server als Open Directory Master konfiguriert sein. Die Datensicherung kann mit wenigen Mausklicks durchgeführt werden (Abbildung 9.1):

1. Starten Sie das Programm Server Admin und verbinden Sie sich mit dem betreffenden Server, der als Open Directory Master arbeitet.
2. Wählen Sie in der Tabelle COMPUTER & DIENSTE den Punkt OPEN DIRECTORY aus.
3. Klicken Sie die Rubrik ARCHIVIEREN am unteren Rand des Fensters an.
4. Geben Sie bei ARCHIVIEREN IN entweder den absoluten Unix-Pfad eines Ordners an, in dem die Datensicherung gespeichert werden soll, oder betätigen Sie die Schaltfläche mit den drei Punkten, um einen Ordner auszuwählen. Beachten Sie, dass Server Admin hierbei auf das lokale Dateisystem desjenigen Servers zugreift, mit dem Sie gerade verbunden sind. Dies muss nicht unbedingt der lokale Computer sein, auf dem Server Admin gerade läuft.
5. Drücken Sie die Schaltfläche ARCHIVIEREN um die Datensicherung zu erstellen.
6. Geben Sie einen Dateinamen für diese Datensicherung in das erscheinende Dialogfenster (Abbildung 9.2) ein. Es empfiehlt sich, einen Namen zu wählen, der das jeweilige Tagesdatum beinhaltet. Ebenso müssen Sie ein Kennwort für die Verschlüsselung der Datensicherung an dieser Stelle eingeben. Denken Sie daran, dass die Open Directory-Daten die sicherheitskritischsten Daten sind, die Ihr Server gespeichert hat, denn es sind unter anderem alle Kennwort-Hashes aller Benutzer im Verzeichnisdienst abgelegt. Sie sollten also ein „gutes“ Kennwort verwenden.

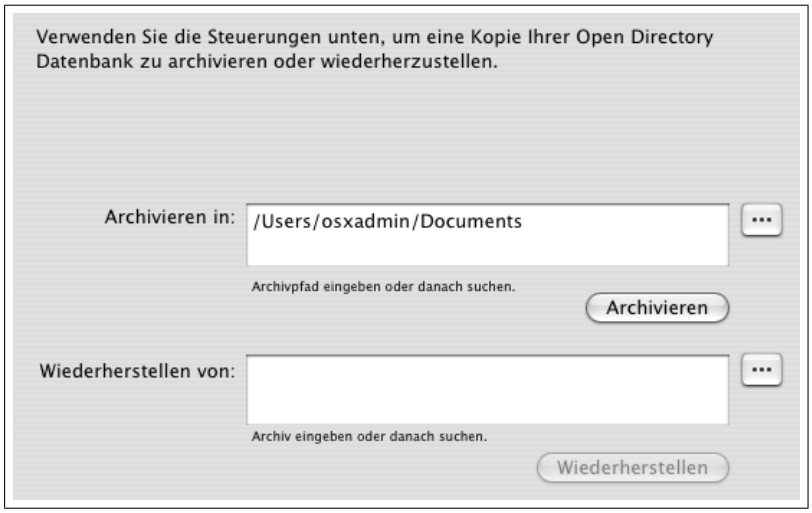
Verwenden Sie die Steuerungen unten, um eine Kopie Ihrer Open Directory Datenbank zu archivieren oder wiederherzustellen.
Archivieren in:
/Users/osxadmin/Documents
Archivpfad eingeben oder danach suchen.
Archivieren
Wiederherstellen von:
Archiv eingeben oder danach suchen.
Wiederherstellen

Abbildung 9.1: Ein neues Feature von Tiger ist das Erstellen einer kompletten Datensicherung aller Open Directory-Daten. Eine Archivkopie kann mit wenigen Mausklicks angelegt werden.

Abbildung 9.2: Die Archivkopie muss mit einem Namen versehen werden und wird mit einem Kennwort verschlüsselt. Da es sich um die kritischsten Sicherheitsdaten des Servers handelt, sollten Sie ein sicheres Kennwort vergeben.

Der Vorgang sollte nach wenigen Minuten beendet sein. Die Archivdatei, die angelegt wird, ist in Wirklichkeit ein verschlüsseltes Mac OS X-Plattenabbild (Disk Image). Es enthält alle Daten, um selbst bei völligem Ausfall eines Server-Computers die Open Directory-Daten auf einem anderen Server wiederherstellen zu können. Unter anderem sind im Archiv enthalten:

- der vollständige Inhalt der LDAP-Datenbank im LDIF-Format
- eine Kopie der lokalen NetInfo-Datenbank des Servers
- eine Kopie aller Kerberos-Schlüsseldaten und der Kerberos-Konfiguration
- eine Kopie der Datenbank des Kennwortservers
- Kopien von allen Dateien, die Shadow-Kennworte enthalten
- Informationen über die gegenwärtige Konfiguration aller Open Directory-Dienste
- Informationen über die Netzwerkkonfiguration des Servers, soweit sie den Betrieb von Open Directory betreffen

Analog kann über die Schaltfläche WIEDERHERSTELLEN eine Archivkopie wieder zurückgeladen werden. Beachten Sie, dass das Zurückladen nur möglich ist, wenn der Server den gleichen Kerberos-Bereichsnamen (Realm) verwendet, wie der Server, auf dem die Archivkopie erstellt wurde. Der Server, auf den zurückgeladen wird, muss (noch) kein Open Directory Master sein, das Zurückladen bewirkt jedoch, dass er danach als Open Directory Master arbeitet. Beim Zurückladen „mischen" sich die Daten aus der Archivkopie mit den momentanen Inhalten der Datenbanken. Dies heißt zum Beispiel, dass bestehende Benutzerkonten nicht gelöscht werden, es sei denn, sie werden durch gleichnamige Konten aus der Datensicherung überschrieben.

Musste ein Open Directory Master über eine Datensicherung wiederhergestellt werden, so geht hierbei die Bindung zwischen Master und Replikatservern verloren. Um dieses Problem zu lösen, sind alle Replikatserver vorübergehend in Open Directory Master umzuwandeln und dann wieder neu als Repliken des eigentlichen Open Directory Masters zu konfigurieren.

9.1.2 Die abgesicherte Bindung zwischen Server und Klienten

Wie in Abschnitt 9.3.1 des Hauptbuchs beschrieben, gibt es ein Sicherheitsrisiko bei der Benutzung von Open Directory, wenn Sie die Client-Computer den LDAP-Server automatisch per DHCP zuweisen lassen und mit einem automatischen Verzeichnissuchpfad arbeiten. Ein möglicher Angreifer könnte nach Eindringen ins Netzwerk einen manipulierten DHCP-Server aufsetzen und damit die Client-Computer auf einen fremden LDAP-Server umleiten, den er selbst mit seinen eigenen Daten installiert hat. Somit können alle Klienten mit manipulierten Sicherheitsinformationen versorgt werden, um damit alle Schutzmaßnahmen im Netz auszuhebeln.

Doch nicht nur das Aufstellen eines gefälschten Servers ist möglich. In umgekehrter Richtung könnte ein Angreifer auch einen manipulierten Client-Computer ins Netz bringen und diesen dazu veranlassen, durch eine Reihe von LDAP-Anfragen an Benutzerdaten, Kontaktdaten und eventuell auch verschlüsselte Kennwort-Hashes zu kommen. Die Hashes könnten dann in einer Offline-Attacke geknackt werden.

In Tiger hat Apple ein zusätzliches Sicherheitsmerkmal integriert: Der Open Directory Server und die Client-Computer können so konfiguriert werden, dass sie sich bei der ersten Kontaktaufnahme identifizieren müssen. Somit wird es für die beteiligten Kommunikationspartner möglich, festzustellen, ob der Computer am anderen Ende der Leitung „echt“ oder „gefälscht“ ist. Technisch läuft dies so ab, dass bei der ersten Kontaktaufnahme zur Bindung eines Klienten an das LDAP-Verzeichnis das Kennwort des Verzeichnisdienstverwalters auf dem Client eingegeben werden muss. Ist das Kennwort richtig, legt der LDAP-Server ein Computerkonto für den Client an, in dem sich ein generierter Hashwert befindet. Bei späteren Kontaktaufnahmen wird dieser Wert als Schlüssel verwendet, um den Client-Computer wieder zu identifizieren.

Auf dem Server kann eingestellt werden, dass dieses Sicherheitsmerkmal auf Wunsch angeboten wird. Zusätzlich kann konfiguriert werden, dass der Server bei der ersten Verbindungsaufnahme auf Eingabe eines Verbindungskennworts besteht.

Leider ist Apples „Lösung“ des Sicherheitsproblems etwas halbherzig: Statt eine zweiseitige gegenseitige Identifikation der Computer bei *jeder* Kontaktaufnahme zum Verzeichnisdienst anzufordern, wird nur die *erste Bindung* zwischen Client und Server authentifiziert. Die Absicherung ist also nicht so sicher, wie man das beim ersten Lesen vermuten könnte. Hinzu kommt, dass alle diesbezüglichen Optionen in der grafischen Oberfläche irreführend beschriftet sind. Dies gilt sowohl für das englische Original als auch für die deutsche Übersetzung, die die Situation noch weiter verschlimmert. Ohne zusätzliche Literatur bleibt die Funktionsweise völlig unverständlich.

Auch der Name dieses neuen Funktionsmerkmals bleibt unklar. In Apples Handbüchern wird es als *vertrauenswürdige Bindung (Trusted Binding)* bezeichnet, in allen Programmen jedoch als *Verzeichnisbindung*. Diese Terminologie widerspricht dem üblichen Sprachgebrauch, bei dem als Verzeichnisbindung die Nutzung eines Verzeichnisdienstes durch einen Klienten bezeichnet wird, wobei der Klient Verwaltungs- und Authentifizierungsdaten des Dienstes übernimmt. Was in Wirklichkeit bei diesem Funktionsmerkmal geschieht, ist eher als *Beitritt zu einer Verzeichnisdienstdomäne* zu bezeichnen. Möglicherweise war dieses Feature von Apple zunächst sehr viel aufwändiger geplant, aber ist dann zurückgezogen worden, weil es nicht rechtzeitig fertiggestellt werden konnte. Die derzeitige Umsetzung der „vertrauenswürdigen Bindung“ hat folgende Konsequenzen:

- Wenn Sie auf dem Server erzwingen, dass Klienten eine vertrauenswürdige Bindung herstellen müssen, brauchen sich bereits eingerichtete Klienten trotzdem nicht zu authentifizieren. Computer, die Ihren LDAP-Server per DH-

CP zugewiesen bekommen, können ohne Prüfung auf die Verzeichnisdienstdaten zugreifen. Ebenso können Klienten, die bereits einen LDAP-Servereintrag im Programm *Verzeichnisdienste* aufweisen, unverändert auf den LDAP-Server zugreifen.

- Die Angriffsmöglichkeit über das Einschmuggeln eines manipulierten DHCP-Servers besteht also weiterhin. Es ist daher zu empfehlen, die Option VOM DHCP-SERVER GELIEFERTE LDAP-SERVER VERWENDEN, UM SUCHPFADE ZU AUTOMATISIEREN auf allen Klienten ausgeschaltet zu lassen.
- Nur wenn ein neuer Klient zum ersten Mal mit dem LDAP-Server verbunden wird, muss beim Fordern einer vertrauenswürdigen Bindung auf dem Client-Computer Name und Kennwort des Verzeichnisdienstadministrators eingegeben werden.
- Nur Klienten mit Mac OS X Tiger oder höher können die Anfrage des Servers nach Eingabe der Authentifizierungsdaten beantworten. Wird die vertrauenswürdige Bindung gefordert, so können ältere Mac OS X-Systeme nicht mehr auf Nutzung des LDAP-Servers eingerichtet werden, es sei denn sie werden per DHCP auf den LDAP-Server verwiesen. Für ältere Systeme, die den LDAP-Server bereits nutzen, ergeben sich keine Änderungen.
- Apple dokumentiert nicht, wie der Server die erfolgreiche Bindung jedem Klienten zuordnet. Hierfür werden die normalen Computerkonten verwendet, die auf Basis der Computernamen (nicht der DNS-Namen!) verwaltet werden. Vorsicht ist geboten, wenn sich Computernamen ändern und auch die richtige Groß- und Kleinschreibung der Namen spielt eine Rolle. Sie können mit dem Arbeitsgruppen-Manager die Computerlisten-Accounts durchsuchen, welche Konten in welcher Namensschreibweise angelegt sind. Schalten Sie den Arbeitsgruppen-Manager auf die Anzeige der LDAP-Rohdaten, können Sie außerdem alle Objekte der Klasse *Computers* überprüfen: Enthalten die Objekte das Attribut *AuthenticationAuthority* (OD-Name *dsAttrTypeNative:authAuthority*), so handelt es sich um „vertrauenswürdig gebundene" Client-Computer.

Um die vertrauenswürdige Bindung auf dem Server möglich zu machen, oder für neu hinzukommende Clients zu erzwingen, führen Sie die folgenden Schritte durch:

1. Starten Sie das Programm Server Admin und verbinden Sie sich mit dem Server, der für diese Verzeichnisdienstdomäne als Open Directory Master arbeitet.
2. Wählen Sie in der Tabelle COMPUTER & DIENSTE den Punkt OPEN DIRECTORY aus.
3. Klicken Sie im unteren Bereich des Fensters auf die Schaltfläche EINSTELLUNGEN, im oberen Bereich auf RICHTLINIEN, dort auf den Unterpunkt BINDUNG.
4. Um möglich zu machen, dass der Server Anfragen von Clients beantwortet, sich per Authentifizierung diesem LDAP-Server zuzuordnen, sorgen Sie dafür, dass der Punkt VERZEICHNISBINDUNG AKTIVIEREN angekreuzt ist.

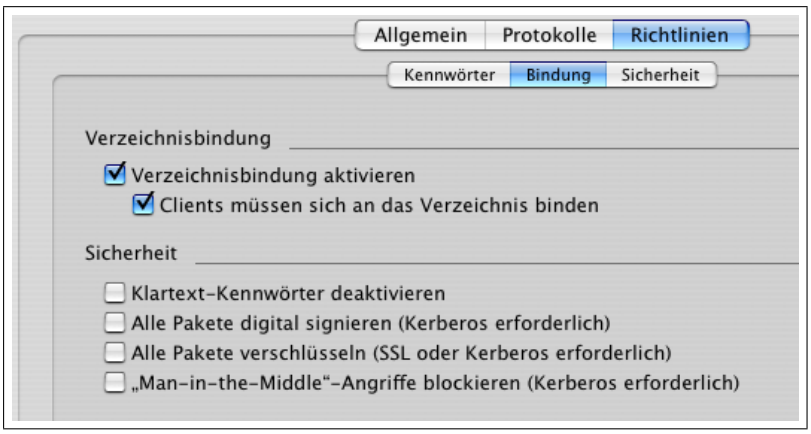

Abbildung 9.3: Apple bezeichnet die vertrauenswürdige Bindung in Server Admin im Moment als Verzeichnisbindung. Das erste Häkchen ermöglicht, das zweite Häkchen erzwingt die Authentifizierung von LDAP-Klienten bei der allerersten Verbindungsaufnahme.

5. Um zusätzlich zu erzwingen, dass neu eingerichtete Clients sich beim ersten Verbindungsaufbau durch Eingabe von Name und Kennwort des Verzeichnisdienstverwalters identifizieren müssen, kreuzen Sie den Punkt CLIENTS MÜSSEN SICH AN DAS VERZEICHNIS BINDEN an.

6. Betätigen Sie die Schaltfläche SICHERN.

Abbildung 9.3 zeigt die neuen Sicherheitsrichtlinien auf der Serverseite. Auf der Seite des Clients richten Sie zunächst wie bisher die Anbindung an den LDAP-Server mit dem Programm *Verzeichnisdienste* ein (siehe Abschnitt 9.3.1 des Hauptbuchs). Geben Sie die IP-Adresse des LDAP-Servers ein, so erscheint jedoch ein erweitertes Eingabefenster (Abbildung 9.4), wenn Mac OS X erkennt, dass der Server die vertrauenswürdige Bindung unterstützt oder sogar erzwingt. Geben Sie wie bereits besprochen den aktuellen Computernamen in korrekter Groß-/Kleinschreibung sowie Name und Kennwort des Verzeichnisdienstverwalters ein. Sind die Daten korrekt, wird das Computerkonto auf dem Server entsprechend eingerichtet, bzw. ergänzt und die LDAP-Verbindung aufgenommen.

9.1.3 Weitere Sicherheitsmerkmale

Neben der Identifizierungsmöglichkeit bei der ersten Kontaktaufnahme zwischen Client und Server, hat Apple in Tiger weitere Sicherheitsrichtlinien eingeführt, die sich gegen das Fälschen von Servern und das Abhören der Netzkommunikation richten. Sie finden die Optionen in der unteren Bildhälfte der neuen Karteikarte BINDUNG (Abbildung 9.3):

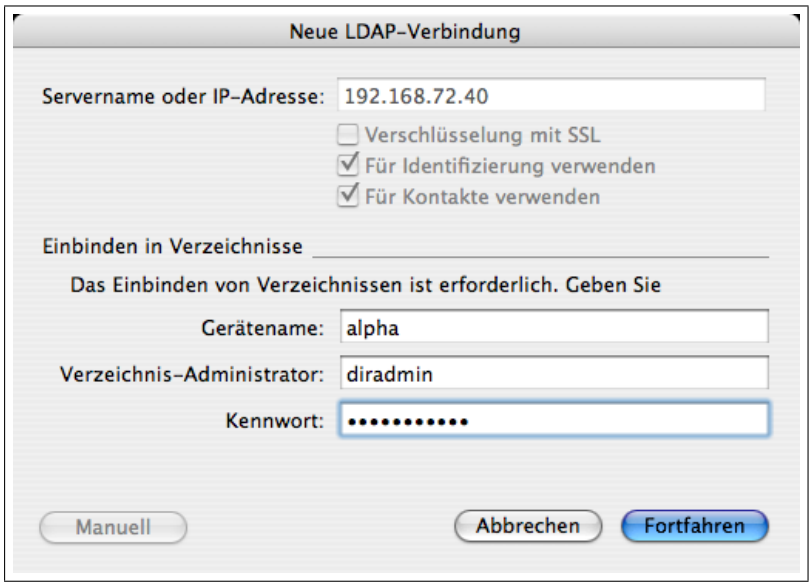

Abbildung 9.4: Die erste Bindung zum Server findet statt. Auf Seiten des Clients lässt die Beschriftung der Optionen noch mehr zu wünschen übrig als auf dem Server. In der deutschen Version ist der Text nicht nur abgeschnitten, sondern auch falsch übersetzt. Achten Sie bei der Eingabe der Daten auf korrekte Groß-/Kleinschreibung.

- Mit der Option KLARTEXT-KENNWÖRTER DEAKTIVIEREN wird die Möglichkeit gesperrt, dass Klienten Anfragen mit unverschlüsselten Kennworten an den Open Directory-Dienst senden können, falls alle Versuche, ein verschlüsseltes Kennwortverfahren auszuhandeln, fehlgeschlagen sind. Beachten Sie diesbezüglich die möglichen Identifizierungsverfahren für den Zugriff auf Open Directory, die bereits in Abschnitt 6.2.2 diskutiert wurden.
- Die Funktion ALLE PAKETE DIGITAL SIGNIEREN steuert, ob beim Datenaustausch zwischen Client und Server alle Daten mit digitalen Unterschriften versehen werden sollen. Wird die Funktion eingeschaltet, kann ein Angreifer, der das Netz abhört, keine Datenpakete abfangen und durch gefälschte Pakete ersetzen.
- Die Auswahl ALLE PAKETE VERSCHLÜSSELN bewirkt, dass ein Angreifer, der das Netz abhört, die Daten nicht mehr mitlesen kann.
- Über die Option „MAN-IN-THE-MIDDLE-ANGRIFFE BLOCKIEREN" werden zusätzliche Sicherheitsmaßnahmen eingeschaltet, die verhindern, dass sich ein Angreifer mit einem eingeschleusten Computer fälschlicherweise als LDAP-Server ausgeben kann. Dieses Funktion sollte immer mit der Funktion ALLE PAKETE DIGITAL SIGNIEREN kombiniert werden.

9.2 Arbeiten mit dem LDAP-Browser

Die Internet-Adresse für den im Hauptbuch vorgestellten LDAP-Browser hat sich inzwischen geändert. Bitte verwenden Sie nun die Adresse

```
http://www-unix.mcs.anl.gov/~gawor/ldap/
```

Bei Redaktionsschluss war Version 2.8.2 Beta 2 die neueste erhältliche Version.

9.3 Arbeiten mit Zertifikaten

9.3.1 Das neu gestaltete Schlüsselbund-Programm

In Mac OS X Tiger hat Apple eine große Zahl neuer Funktionen eingeführt, die den Umgang mit Zertifikaten erleichtern. Dies betrifft sowohl die Standardversion als auch die Serverversion. Zertifikate, Zertifikatsaussteller sowie deren private und öffentliche Schlüssel können nun zentral über das Programm *Schlüsselbund* eingesehen und verändert werden, ohne dass man als Benutzer wissen muss, welche Dateien dahinter stecken und wo sie sich befinden.

Um einen Eindruck hiervon zu bekommen, starten Sie das Programm *Schlüsselbund* (im Ordner *Dienstprogramme*) und betätigen Sie die Schaltfläche SCHLÜSSELBUNDE EINBLENDEN links unten, falls der linke Teil des Fensters nicht aus zwei Tabellen

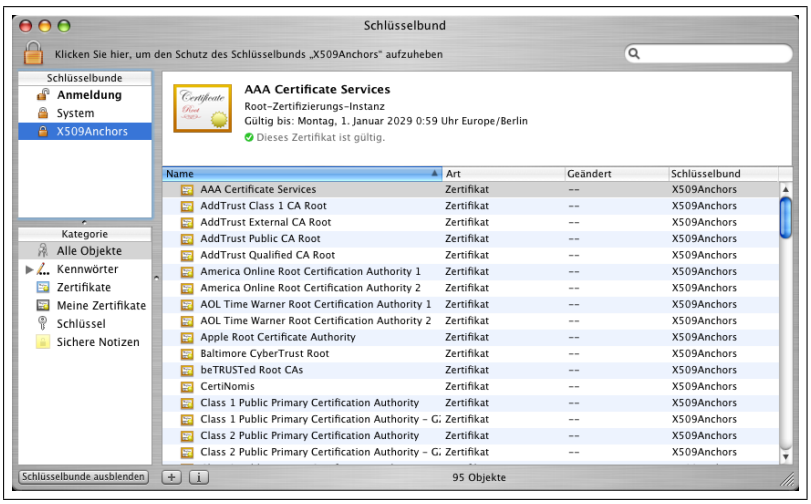
Schlüsselbund
Klicken Sie hier, um den Schutz des Schlüsselbunds „X509Anchors" aufzuheben
Schlüsselbunde
Anmeldung
System
X509Anchors
Kategorie
Alle Objekte
Kennwörter
Zertifikate
Meine Zertifikate
Schlüssel
Sichere Notizen
AAA Certificate Services
Root-Zertifizierungs-Instanz
Gültig bis: Montag, 1. Januar 2029 0:59 Uhr Europe/Berlin
Dieses Zertifikat ist gültig.
Name
Art
Geändert
Schlüsselbund
AAA Certificate Services Zertifikat -- X509Anchors
AddTrust Class 1 CA Root Zertifikat -- X509Anchors
AddTrust External CA Root Zertifikat -- X509Anchors
AddTrust Public CA Root Zertifikat -- X509Anchors
AddTrust Qualified CA Root Zertifikat -- X509Anchors
America Online Root Certification Authority 1 Zertifikat -- X509Anchors
America Online Root Certification Authority 2 Zertifikat -- X509Anchors
AOL Time Warner Root Certification Authority 1 Zertifikat -- X509Anchors
AOL Time Warner Root Certification Authority 2 Zertifikat -- X509Anchors
Apple Root Certificate Authority Zertifikat -- X509Anchors
Baltimore CyberTrust Root Zertifikat -- X509Anchors
beTRUSTed Root CAs Zertifikat -- X509Anchors
CertiNomis Zertifikat -- X509Anchors
Class 1 Public Primary Certification Authority Zertifikat -- X509Anchors
Class 1 Public Primary Certification Authority – G. Zertifikat -- X509Anchors
Class 2 Public Primary Certification Authority Zertifikat -- X509Anchors
Class 2 Public Primary Certification Authority – G. Zertifikat -- X509Anchors
Schlüsselbunde ausblenden
95 Objekte

Abbildung 9.5: Das Schlüsselbund-Programm hat in Tiger eine komplett neue Benutzeroberfläche bekommen. Bei der Arbeit mit Zertifikaten stellt es eine große Vielzahl neuer Funktionen bereit.

besteht. Die obere Tabelle zeigt die Liste der aktiven Schlüsselbunde, die vom aktuellen Benutzer-Account aus zugreifbar sind, die untere Tabelle die Informationskategorien, die innerhalb des ausgewählten Schlüsselbunds genutzt werden können (Abbildung 9.5).

In der Rolle des Verwalters sollten Ihnen mindestens drei Schlüsselbunde angezeigt werden: Ihr eigener Schlüsselbund, der entweder unter dem Stichwort *Anmeldung* oder unter Ihrem Kurznamen angezeigt wird, der Schlüsselbund dieses Computers, der als *System* angezeigt wird und schließlich ein spezieller Schlüsselbund, der mit dem Namen *X509Anchors* versehen ist. In diesem speziellen Schlüsselbund sind ausschließlich Zertifikate enthalten, nämlich solche, die die Echtheit von weltweit bekannten Zertifikatsausstellern *(Certificate Authorities, CAs)* bestätigen. Auch Apple selbst ist in der Liste enthalten.

Wie im Hauptbuch in Abschnitt 9.5.1 erläutert, beruht die Funktion von Zertifikaten darauf, dass sie jeweils von einer Partei digital unterschrieben wurden, deren Identität wiederum von einer anderen Partei durch digitale Unterschrift bestätigt wurde. Es bildet sich eine Kette von Echtheitsbestätigungen, an deren oberem Ende eine Zertifizierungsstelle stehen muss, deren Echtheit man vertraut. Diese Kette von Bestätigungen wird über einen Austausch digitaler öffentlicher Schlüssel nach der Norm X.509 verwaltet, das Ende der Kette bildet einen „festen Anker", deshalb die Bezeichnung *X509Anchors*. Ein solcher Anker ist damit die oberste, letzte Instanz, um die Echtheit eines Zertifikats bestätigen zu können. Die entsprechende Zertifizierungsstelle wird als *Root Certificate Authority* bezeichnet, von Apple als *Root-Zertifizierungs-Instanz* übersetzt.

Wenn Sie ein Zertifikat in der Liste anklicken, werden sämtliche Detaildaten über

Apple Root Certificate Authority
Apple Root Certificate Authority
Root-Zertifizierungs-Instanz
Gültig bis: Montag, 10. Februar 2025 1:18 Uhr Europe/Berlin
Dieses Zertifikat ist gültig.
Details
Betreff
Land US
Organisation Apple Computer, Inc.
Organisationseinheit Apple Computer Certificate Authority
Allgemeiner Name Apple Root Certificate Authority
Name des Ausstellers
Land US
Organisation Apple Computer, Inc.
Organisationseinheit Apple Computer Certificate Authority
Allgemeiner Name Apple Root Certificate Authority
Version 3
Seriennummer 1
Signaturalgorithmus SHA-1 mit RSA-Verschlüsselung (1 2 840 113549 1 1 5)
Parameter Ohne

Abbildung 9.6: Auch Apple selbst ist in der Liste der mitgelieferten Zertifikate als letzte Instanz der Beglaubigungskette enthalten. Das Schlüsselbundprogramm kann sämtliche Details des Zertifikats anzeigen.

Abbildung 9.7: Möchten Sie die Sicherheitsrichtlinien bei der Verwendung von Zertifikaten weiter einschränken, können Sie das im unteren Bereich des Zertifikatsfensters vornehmen.

Aussteller, Version, digitale Unterschriften und Verwendungsmöglichkeiten angezeigt (Abbildung 9.6). Am Ende des Zertifikatsfensters befinden sich – mit einem Aufdeckungspfeil unter dem Stichwort EINSTELLUNGEN BESTÄTIGEN gruppiert – die von Ihnen einstellbaren Richtlinien, nach denen das ausgewählte Zertifikat auf diesem Computer verwendet werden darf. Genauer gesagt können Sie mit den Einstellungen festlegen, für welche Anwendungen Mac OS X dem Zertifikat trauen darf und für welche nicht. Sie können für jede Verwendungsmöglichkeit eines Zertifikats zwischen den folgenden vier Möglichkeiten entscheiden (Abbildung 9.7):

- **Systemeinstellungen verwenden:** Sie verwenden die in Mac OS X eingebaute Sicherheitsrichtlinie, um dieses Zertifikat zu prüfen. Dies wird im nächsten Absatz noch detailliert erläutert.
- **Immer vertrauen:** Sie akzeptieren dieses Zertifikat grundsätzlich als echt, sofern Mac OS X von sich aus nicht schon strengere Prüfungsrichtlinien vorschreibt.
- **Genehmigung einholen:** Mac OS X soll bei jeder Verwendung dieses Zertifikats anfragen, ob Sie es als vertrauenswürdig anerkennen.
- **Nie vertrauen:** Sie vertrauen diesem Zertifikat grundsätzlich nicht.

Mit dem obersten Klappmenü BEI VERWENDUNG DIESES ZERTIFIKATS können Sie die Einstellungen für alle möglichen Anwendungsfälle der Zertifikats *gleichzeitig* ändern. Die Verwendungsmöglichkeiten und die jeweils als Systemeinstellungen vorgesehenen Sicherheitsrichtlinien lauten wie folgt:

- SECURE SOCKETS LAYER (SSL): Der Name, der im Zertifikat genannt ist, muss mit mindestens einem DNS-Namen des Computers übereinstimmen, zu dem eine Verbindung mit SSL aufgenommen wird. SSL-Client-Zertifikate sind hiervon ausgenommen. Ist im Zertifikat das Feld ERWEITERTE SCHLÜSSELVERWENDUNG vorhanden, so muss dieses einen gültigen Wert besitzen.
- S/MIME (SECURE MAIL): Um eine Mail digital unterzeichnen oder verschlüsseln zu können, muss die E-Mail-Adresse des Benutzers im Zertifikat aufgeführt sein. Außerdem müssen alle Felder für Schlüsselverwendung im Zertifikat vorhanden sein, die für das Absichern einer E-Mail-Nachricht nötig sind.
- EAP (EXTENSIBLE AUTHENTICATION): Der Name, der im Zertifikat genannt ist, muss mit mindestens einem DNS-Namen des Computers übereinstimmen, zu dem eine Verbindung über ein Netzwerk aufgenommen wird, das eine Identifizierung gemäß der Norm *IEEE 802.1X* anfordert. Client-Zertifikate sind hiervon ausgenommen. Ist im Zertifikat das Feld ERWEITERTE SCHLÜSSELVERWENDUNG vorhanden, so muss dieses einen gültigen Wert besitzen.
- CODE-SIGNIERUNG: Im Zertifikat müssen alle Felder für Schlüsselverwendung vorhanden sein, die zum Signieren von Code nötig sind.
- IP SECURITY (IPSEC): Der Name, der im Zertifikat genannt ist, muss mit mindestens einem DNS-Namen des Computers übereinstimmen, zu dem eine Verbindung über ein Netzwerk aufgenommen wird, das eine Identifizierung gemäß IPSec-Standard anfordert. Client-Zertifikate sind hiervon ausgenommen. Ist im Zertifikat das Feld ERWEITERTE SCHLÜSSELVERWENDUNG vorhanden, so muss dieses einen gültigen Wert besitzen.
- ICHAT-SICHERHEIT: Im Zertifikat müssen alle Felder für Schlüsselverwendung vorhanden sein, die für die Nutzung von iChat nötig sind.
- X.509 STANDARD POLICY: Die Echtheit dieses Zertifikats muss anhand einer X.509-Bestätigungskette nachgewiesen werden können, wobei der Zertifikatsaussteller am Ende der Kette in der Liste X509ANCHORS enthalten sein muss.

9.3.2 Ungültigwerden von Zertifikaten

Aus den gleichen Gründen, aus denen ein Reisepass nur ein paar Jahre gültig bleibt, hat auch ein Zertifikat immer nur eine begrenzte Gültigkeitsdauer. Gültigkeit und Überprüfungsergebnis werden nach Auswählen eines Zertifikats im oberen Bereich des Schlüsselbundfensters angezeigt (siehe Abbildung 9.6). Neben dem voreingestellten Verfallsdatum jedes Zertifikats kann es aber auch andere Gründe geben, weshalb ein Zertifikat ungültig werden kann: Es könnte sein, dass ein anderes Zertifikat, das die Echtheit eines Glieds in der Beglaubigungskette bescheinigt, abgelaufen ist. In dem Fall können alle von dieser Partei unterzeichneten Zertifikate ebenfalls nicht mehr als beglaubigt anerkannt werden. Auch kann die Firma des Zertifikatsausstellers erloschen sein oder beim Aussteller wurde eine Sicherheitslücke entdeckt, so dass dieser Aussteller nicht mehr als vertrauenswürdig erscheint.

Für erhöhte Sicherheitsanforderungen ist es deshalb notwendig, nicht nur das Gültigkeitsdatum eines aktuell vorgelegten Zertifikates zu prüfen, sondern das Gleiche auch für alle Zertifikate der Vorinstanzen der Beglaubigungskette bis hin zur Root-Zertifizierungs-Instanz zu tun und hierbei auch auf *zurückgezogene Zertifikate* zu prüfen. Ob ein Zertifikat einer Vorinstanz offiziell als zurückgezogen gilt, kann durch eine Sicherheitsüberprüfung über das Internet festgestellt werden. Hierfür haben sich zwei Standards etabliert:

- **OCSP:** OCSP ist die Abkürzung für *Online Certificate Status Protocol* und bezeichnet die Möglichkeit, bei jedem einzelnen Zertifikat durch eine Abfrage im Internet herausfinden zu können, ob es eventuell zurückgezogen wurde.

- **CRL:** CRL bezeichnet die *Certificate Revocation List* und bezieht sich auf eine im Internet gewartete Gesamtliste, die alle Zertifikate enthält, die jemals zurückgezogen wurden.

Die Arbeitsweise von OCSP ist mit der eines DNS-Servers vergleichbar: Ein Client sendet eine kurze Anfrage an OCSP, ob ein gegebenes Zertifikat gültig ist, und ein OCSP-Server liefert eine simple Rückantwort mit den Möglichkeiten *gültig*, *abgelaufen* oder *unbekannt*. CRL arbeitet dagegen ähnlich wie ein Web-Server, von dem man ein Dokument herunterlädt: Die Liste der zurückgezogenen Zertifikate wird vom Client angefordert, herunterkopiert und durch Durchsuchen der Liste kann der Client feststellen, ob ein gegebenes Zertifikat gültig ist. Wahrscheinlich erkennen Sie, dass OCSP gegenüber CRL das elegantere System ist. Man schätzt, dass sich auf absehbare OCSP als Prüfungsverfahren durchsetzen wird.

Um OCSP, CRL oder beide Verfahren in Mac OS X nutzen zu können, brauchen Sie nur eine Einstellung im Schlüsselbund zu ändern (Abbildung 9.8):

1. Rufen Sie im Programm Schlüsselbund den Menüpunkt SCHLÜSSELBUND | EINSTELLUNGEN auf.

2. Wählen Sie die Rubrik ZERTIFIKATE aus.

3. Wählen Sie in den Klappmenüs für OCSP und CRL jeweils die von Ihnen gewünschte Sicherheitsrichtlinie aus. Sie können entweder keine Prüfung auf zurückgezogene Zertifikate durchführen (AUS), versuchen, eine Prüfung durchzuführen, aber falls die Prüfung kein schlüssiges Ergebnis liefert, das Zertifikat trotzdem akzeptieren (BESTER VERSUCH), die Prüfung immer dann durchführen, falls im Zertifikat ein entsprechender Vermerk angegeben ist (ERFORDERLICH, FALLS IM ZERTIFIKAT ANGEGEBEN) oder generell erzwingen, dass alle Zertifikate streng geprüft werden müssen (FÜR ALLE ZERTIFIKATE ERFORDERLICH).

4. Über den Punkt PRIORITÄT können Sie einstellen, ob OCSP oder CRL der Vorzug gegeben werden soll, beziehungsweise, ob sogar beide Verfahren herangezogen werden müssen, bevor ein Zertifikat als gültig anerkannt wird.

Abbildung 9.8: Sie können die Sicherheitseinstellungen weiter erhöhen, indem Sie die Verfahren OCSP und CRL nutzen, um Zertifikate auf zurückgezogene Beglaubigungen zu prüfen.

Weitere interessante Einstellungen bezüglich der Zertifikate finden Sie unter der Rubrik ALLGEMEIN: Apple hat hier vorgesehen, dass Zertifikate nicht nur auf der lokalen Platte, sondern auch über den .Mac-Dienst oder über den Verzeichnisdienst Ihres Netzwerks gesucht werden sollen.

9.3.3 Erzeugen eines Spielzertifikats zum SSL-Zugriff auf den LDAP-Server

Wir hatten in Abschnitt 9.5.2 des Hauptbuchs festgehalten, wie Sie mithilfe der Kommandozeile ein selbst unterzeichnetes Zertifikat erstellen können, beispielsweise um auf einem Mac OS X Server einen abgesicherten SSL-Zugriff auf den LDAP-Server realisieren zu können. Dank der neuen Funktionen in Tiger ist hierzu die Kommandozeile nicht mehr erforderlich. Wir zeigen im Folgenden am gleichen Beispiel, wie Sie diese Aufgabe mit einem 10.4-Server lösen können.

1. Starten Sie das Programm *Server Admin* und verbinden Sie sich mit dem Server, der den LDAP-Dienst beherbergt, der mit SSL abgesichert werden soll.
2. Wählen Sie auf der linken Seite des Fensters in der Tabelle COMPUTER & DIENSTE den Namen des Servers aus und gehen Sie auf der rechten Seite in den Punkt EINSTELL..
3. Öffnen Sie die Rubrik ZERTIFIKATE.
4. Drücken Sie die Schaltfläche mit dem Pluszeichen unterhalb der Tabelle, um ein neues Zertifikat anzulegen. Es erscheint eine Eingabemaske wie in Abbildung 9.9, die Sie ausfüllen müssen. Beachten Sie, dass im unteren Teil der

Text INSTANZ: SELBST SIGNIERT angegeben ist. Wir erstellen also ein Zertifikat, bei dem wir uns selbst beglaubigen (siehe auch Abbildung 9.9).

5. Geben Sie bei ALLGEMEINGÜLTIGER NAME den DNS-Namen des LDAP-Servers an, der auf SSL umgestellt werden soll. Es muss der voll qualifizierte Domänenname (FQDN) angegeben werden. Dies ist wichtig, denn wie im vorigen Abschnitt erläutert, ist die voreingestellte Sicherheitsrichtlinie in Tiger, den Namen des Zertifikats gegen den DNS-Namen des Servers zu prüfen.

6. Füllen Sie die übrigen Felder mit den Daten Ihrer Organisation aus.

7. Geben Sie bei GÜLTIG BIS das gewünschte Ablaufdatum des Zertifikats an. Mac OS X schlägt als Startdatum das Tagesdatum und als Gültigkeitsdauer ein Jahr vor.

8. Lassen Sie das Feld PRIVATE SCHLÜSSELLÄNGE auf der Standardeinstellung und geben Sie bei SCHLÜSSELKENNWORT nichts ein. Dies vermeidet eventuelle Kompatibilitätsprobleme mit dem LDAP-Server.

9. Betätigen Sie die Schaltfläche SICHERN. Die Erstellung des Zertifikats kann einige Sekunden Rechenzeit benötigen.

10. Gehen Sie mit dem Pfeilknopf links oben auf die Zertifikatstabelle zurück. Das neue Zertifikat wird angezeigt.

Wenn Sie den oben beschriebenen Ablauf einmal ausprobieren, werden Sie sehen, dass auch im Programm Schlüsselbund das neue Zertifikat und dessen Schlüssel sofort sichtbar werden. Wählen Sie hierzu den Schlüsselbund SYSTEM aus. In der Kategorie ALLE OBJEKTE werden sowohl das neue Zertifikat als auch der öffentliche und private Schlüssel, die zum Zertifikat gehören, angezeigt (Abbildung 9.10). Das im Hauptbuch angegebene manuelle Handling von pem-Dateien ist in Tiger nicht mehr erforderlich.

Nun müssen Sie nur noch das Open Directory-System so konfigurieren, dass SSL auf Basis des neuen Zertifikats zum Einsatz kommt.

1. Wechseln Sie zurück ins Programm Server Admin und wählen Sie den Dienst OPEN DIRECTORY aus.

2. Öffnen Sie die Rubrik EINSTELLUNGEN.

3. Wählen Sie die Karteikarte PROTOKOLLE aus.

4. Setzen Sie im unteren Bereich das Häkchen beim Punkt SSL (SECURE SOCKETS LAYER) AKTIVIEREN

5. Wählen Sie im Klappmenü das soeben erstellte ZERTIFIKAT aus.

6. Betätigen Sie die Schaltfläche SICHERN.

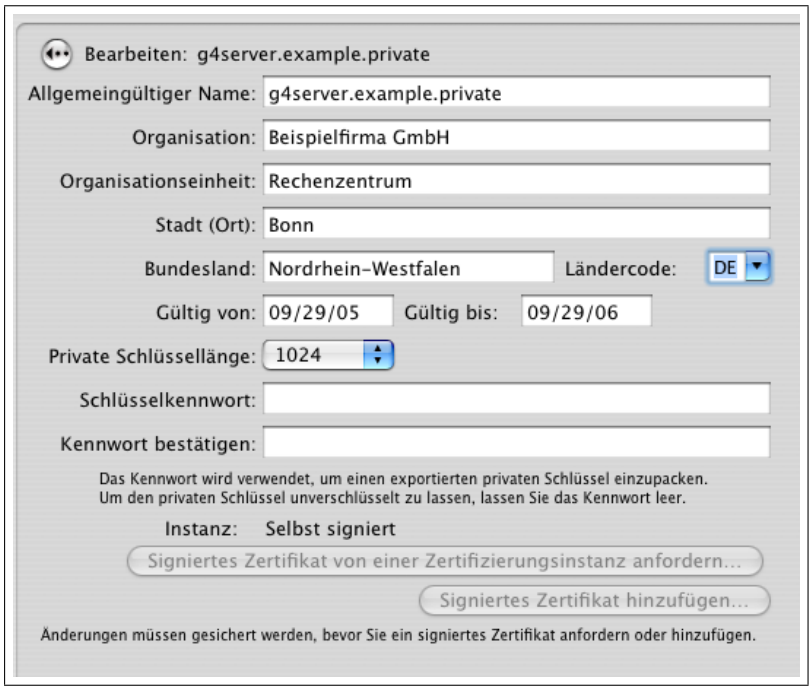
Bearbeiten: g4server.example.private
Allgemeingültiger Name: g4server.example.private
Organisation: Beispielfirma GmbH
Organisationseinheit: Rechenzentrum
Stadt (Ort): Bonn
Bundesland: Nordrhein-Westfalen
Ländercode: DE
Gültig von: 09/29/05
Gültig bis: 09/29/06
Private Schlüssellänge: 1024
Schlüsselkennwort:
Kennwort bestätigen:
Das Kennwort wird verwendet, um einen exportierten privaten Schlüssel einzupacken.
Um den privaten Schlüssel unverschlüsselt zu lassen, lassen Sie das Kennwort leer.
Instanz: Selbst signiert
Signiertes Zertifikat von einer Zertifizierungsinstanz anfordern...
Signiertes Zertifikat hinzufügen...
Änderungen müssen gesichert werden, bevor Sie ein signiertes Zertifikat anfordern oder hinzufügen.

Abbildung 9.9: Dank der neuen Zertifikatsfunktionen lässt sich auf dem Server per Knopfdruck ein selbst signiertes Zertifikat erstellen, das zur Absicherung des LDAP-Servers über SSL genutzt werden kann.

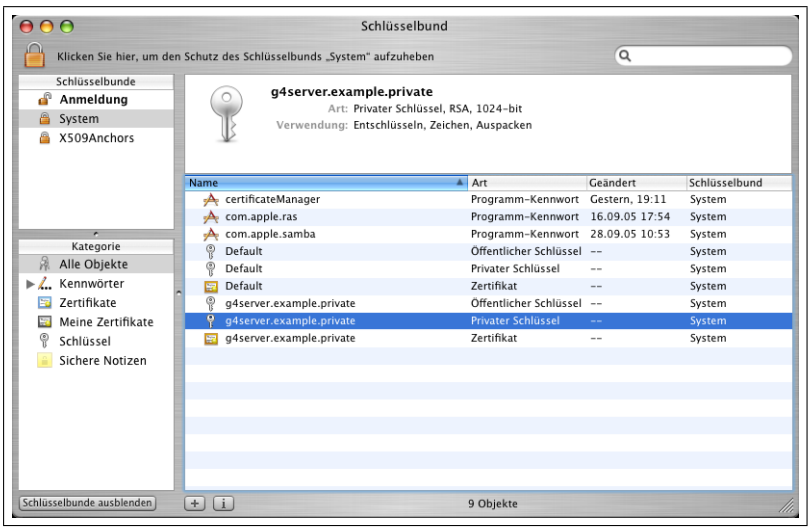

Abbildung 9.10: Das neu erstellte Zertifikat und dessen Schlüssel werden sofort verfügbar, ohne dass ein Importieren oder Exportieren der Daten oder das Kopieren von pem-Dateien erforderlich ist.

Vorsicht: Denken Sie daran, dass Sie auch alle Klienten im Netz auf SSL umstellen müssen. Für den Fall, dass Sie den LDAP-Server automatisch per DHCP konfigurieren, ist die Vorgehensweise im Hauptbuch beschrieben. Bei manueller Konfiguration müssen Sie mit dem Programm *Verzeichnisdienste* auf jedem Client-Computer unter LDAPv3 | KONFIGURIEREN... das Feld SSL ankreuzen.

Die Verzeichnisdienstklienten werden das Zertifikat des LDAP-Server problemlos akzeptieren. Zeigen Sie die Daten des soeben erstellten Zertifikats jedoch im Schlüsselbund-Programm an, oder versuchen Sie, sich über den in Abschnitt 9.2 erwähnten LDAP-Browser per SSL zu verbinden, so funktioniert zwar auch das, aber Sie werden mit unschönen Sicherheitswarnungen konfrontiert (Abbildungen 9.11 und 9.12). Den Programmen ist bewusst, dass das benutzte Zertifikat nur von Jemandem unterzeichnet wurde, der nicht durch eine Root-Zertifizierungs-Instanz beglaubigt wurde. Wir nutzen diesen Effekt, um im nächsten Abschnitt auf weitere neue Fähigkeiten von Tiger einzugehen.

9.3.4 Eine private Zertifizierungsstelle einrichten

In größeren Betrieben, Schulen oder Universitäten ist es in der Regel kaum machbar, die Netzwerkhardware physisch abhörsicher einzurichten. Gerade hier ist aber die Gefahr böswilliger Angriffe – auch aus dem eigenen Hausnetz heraus – gegeben. Von daher ist es durchaus üblich, das eigene Netz durch Einsatz von Verschlüsselungs- und Signatur-Verfahren mithilfe von Zertifikaten abzusichern. Doch beglaubigte Zertifikate, die jedes Jahr erneuert werden müssen, sind besonders für

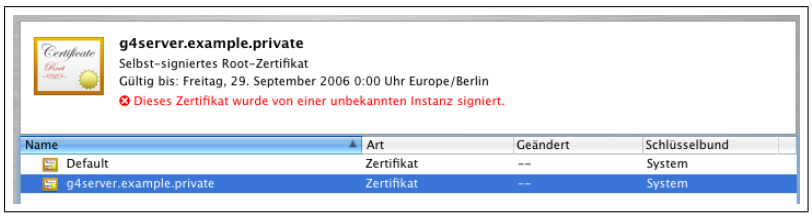

Abbildung 9.11: Mac OS X weiß, dass das selbst erstellte Zertifikat nicht von einer höheren Zertifizierungsstelle beglaubigt wurde. Im Schlüsselbund wird eine rote Warnmeldung angezeigt.

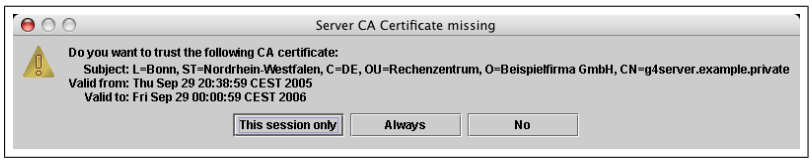
Server CA Certificate missing
Do you want to trust the following CA certificate:
Subject: L=Bonn, ST=Nordrhein-Westfalen, C=DE, OU=Rechenzentrum, O=Beispielfirma GmbH, CN=g4server.example.private
Valid from: Thu Sep 29 20:38:59 CEST 2005
Valid to: Fri Sep 29 00:00:59 CEST 2006
This session only
Always
No

Abbildung 9.12: Auch der LDAP-Browser ist vorsichtig und fragt an, ob er einem nicht beglaubigten Zertifikat trauen soll.

Schulen ein teurer Luxus. Und der Einsatz von selbst signierten Zertifikaten kann zu unerwünschten Warnmeldungen in Programmen führen, wie wir oben gezeigt haben.

Auch hierfür gibt es eine kostengünstige Lösung, die in Mac OS X 10.4 mit wenigen Schritten eingerichtet werden kann: Sie erstellen ein selbst signiertes Zertifikat, das Sie selbst als Zertifizierungsstelle ausweist und weisen alle Rechner in Ihrem Hausnetz an, dieses Zertifikat als gültige Root-Zertifizierungs-Instanz *(Root CA)* anzuerkennen. In den Augen Ihrer eigenen Computer werden Sie damit zu einem gültigen Zertifikatsaussteller. Zwar sind Sie nicht wirklich offiziell beglaubigt, aber Sie können Ihr eigenes Netz dazu bringen, dem Zertifikat trotzdem zu trauen, indem Sie das Zertifikat in die Liste der X509Anchors einfügen. Auf Basis dieses Primärzertifikats können Sie dann selbst beliebig viele weitere Zertifikate zur Verwendung in Ihrem Haus – für den LDAP-Server, den Intranet-Webserver, den SMTP-Server, den POP/IMAP-Server, etc. – erzeugen. Die Klienten trauen diesen Zertifikaten dann automatisch und ohne weitere Warnung, denn es ist ja eine gültige Beglaubigungsinstanz bekannt.

Es sei noch einmal darauf hingewiesen, dass alle diese Zertifikate nur für den privaten Einsatz geeignet sind. Sobald mit diesen Zertifikaten signierte Daten nach außen gelangen, z.B. wenn Sie solch ein Zertifikat für einen HTTPS-Web-Server einsetzen, der aus dem Internet heraus erreichbar ist, werden die Empfänger der Daten Warnmeldungen bekommen, dass dem Absender nicht vertraut werden kann.

Um ein Zertifikat zu erstellen, dass uns als Root-Zertifizierungs-Instanz ausweist, verwenden wir ein weiteres neues Programm von Tiger, den *Zertifikatsassistenten*. Er wird gestartet, indem man im Programm Schlüsselbund den Menüpunkt

SCHLÜSSELBUND | ZERTIFIKATSASSISTENT aufruft. Bevor wir das tun, um die Einrichtung der Zertifizierungsinstanz durchzuspielen, erstellen Sie bitte zunächst einen neuen Schlüsselbund. Das Anlegen eines neuen Schlüsselbunds ist sinnvoll, um unser Primärzertifikat und die danach ausgestellten weiteren Zertifikate sowie alle dazugehörigen Schlüssel sauber unter einem Stichwort gruppieren zu können.

1. Melden Sie sich auf dem Server-Computer als Benutzer *root* an. Die Administrator-Kennung reicht für einige der folgenden Schritte nicht aus. Sie müssen als root-Benutzer arbeiten.
2. Starten Sie das Programm Schlüsselbund.
3. Rufen Sie den Menüpunkt ABLAGE | NEUER SCHLÜSSELBUND... auf.
4. Geben Sie den Namen des neuen Schlüsselbunds, z.B. *Privatzertifikate* ein und drücken Sie die Taste ERSTELLEN...
5. Vergeben Sie ein Kennwort für den neuen Schlüsselbund im darauffolgenden Dialogfenster.
6. Rufen Sie den Menüpunkt SCHLÜSSELBUND | ZERTIFIKATSASSISTENT auf.
7. Der Assistent begrüßt Sie zunächst mit einem Fenster *Einführung*. Durch Druck auf FORTFAHREN wird der eigentliche Dialog gestartet.
8. Wählen Sie den Punkt EINE ZERTIFIZIERUNGSINSTANZ ERSTELLEN aus und drücken Sie auf FORTFAHREN.
9. Es erscheint die Eingabemaske *Zertifikatsinformationen* ähnlich wie in Abbildung 9.13. Lassen Sie den Punkt ZERTIFIKAT WIRD „SELBST-SIGNIERT" (WURZEL) angekreuzt und füllen Sie alle Felder der Maske mit Ihren Daten aus. Als ALLGEMEINER NAME sollte Ihr Firmen- oder Schulname angegeben werden. Anders als im vorigen Abschnitt muss es sich nicht um einen DNS-Namen handeln, denn wir stellen ja kein Zertifikat für die Identität eines Server-Computers aus, sondern bescheinigen uns selbst unsere eigene Identität.
10. Lassen Sie das Feld SERIENNUMMER auf 1 stehen und geben Sie bei GÜLTIGKEITSDAUER die gewünschte Dauer an. Da wir das Zertifikat nur für Privatzwecke benutzen können, kann die Gültigkeitsdauer ruhig sehr hoch sein. Drücken Sie auf FORTFAHREN.
11. Sie können die nächsten sechs Dialogfenster jeweils auf Standardwerten belassen und auf FORTFAHREN drücken, bis der Punkt ORT FÜR DAS ZERTIFIKAT ANGEBEN erscheint.
12. Wählen Sie in diesem Dialog den Schlüsselbund aus, den wir gerade neu eingerichtet haben und drücken Sie auf FORTFAHREN.
13. Veranlassen Sie im nächsten Dialogfenster die Erstellung des neuen Zertifikats. Sie sollten den vorgeschlagenen Namen übernehmen und das Feld DIESE ZERTIFIZIERUNGSINSTANZ ALS STANDARD VERWENDEN angekreuzt lassen.

14. Das Zertifikat und die zugehörigen Schlüssel werden erstellt, was einige Sekunden dauern kann. Der Assistent zeigt abschließend eine Zusammenfassung. Sie können den Assistenten beenden.

Im neuen Schlüsselbund finden Sie nun das neue Zertifikat mit dessen privaten und öffentlichen Schlüsseln. Wenn Sie das Zertifikat auswählen, wird wieder eine Warnung angezeigt, dass das Zertifikat von einem unbekannten Aussteller unterschrieben wurde. Dies ist korrekt. Wir müssen diesem und allen weiteren Computern Ihres Netzes nun beibringen, dass wir „uns selbst trauen können", indem wir das Zertifikat in die Liste der X509Anchors übertragen.

1. Ziehen Sie mit der Maus das neue Zertifikat nach links über den Schlüsselbund X509ANCHORS. Es ist nicht wichtig, ob das Schlosssymbol geöffnet ist.

2. Beenden Sie das Programm Schlüsselbund.

3. Starten Sie das Programm Schlüsselbund wieder neu.

4. Gehen Sie zum Schlüsselbund X509ANCHORS und wählen Sie das neue Zertifikat aus.

Wenn alles geklappt hat, ist das neues Zertifikat jetzt mit einem grünen Häkchen als gültig markiert (Abbildung 9.14). Wir sind erfolgreich zu unserer eigenen Zertifizierungsstelle geworden! Die Dateien, die hierzu angelegt wurden, befinden sich übrigens im Ordner

```
/var/root/Library/Application Support/Certificate Authority
```

Nun müssen allerdings noch alle anderen Klienten im Netz, die unsere Zertifikate nutzen möchten, ebenso bestätigen, dass sie dieser nicht offiziell akkreditierten Zertifizierungsstelle trauen sollen. Auch dort muss das CA-Zertifikat in die Liste der X509Anchors eingetragen werden. Dies lässt sich zum Beispiel so realisieren, dass das Zertifikat per Verzeichnisdienst oder E-Mail an andere Nutzer weitergeleitet wird. Die einfachste Lösung ist natürlich die Verteilung über den File-Server. Wir zeigen dies im folgenden Beispiel, das auch noch einmal veranschaulicht, wie auf Basis der neuen Zertifizierungsinstanz eigene Zertifikate ausgestellt werden.

Erstellen eigener Zertifikate

Wir nehmen an, dass Ihr Server-Computer als POP-Mailserver arbeitet und erstellen im folgenden Beispiel ein neues Zertifikat, um eine SSL-gesicherte Verbindung mit dem POP-Dienst aufbauen zu können.

Abbildung 9.13: Das Zertifikat für die eigene Root-Zertifizierungs-Instanz wird ausgefüllt.

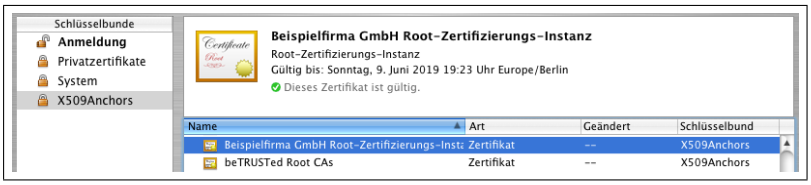

Abbildung 9.14: Das Schlüsselbund-Programm bestätigt, dass wir nun ein gültiges Zertifikat haben, das uns selbst als Root-Zertifizierungs-Instanz ausweist.

Der Zertifikatsassistent hat einen Programmierfehler in der Benutzeroberfläche: Sobald Sie das Fenster geschlossen haben, bekommen Sie kein neues mehr auf. Sie müssen das Assistentenprogramm beenden und es dann entweder über den Schlüsselbund oder über `/System/Library/CoreServices/Certificate Assistent.app` neu starten.

1. Sie müssen immer noch als *root* angemeldet sein. Öffnen Sie den Zertifikatsassistenten erneut und wählen Sie im zweiten Dialogfenster OPTIONEN den Punkt EIN EIGENES ZERTIFIKAT ERSTELLEN aus.

2. Füllen Sie wieder das Formular ZERTIFIKATIONSINFORMATIONEN mit Ihren Daten aus. Hierbei ist wichtig, dass als ALLGEMEINER NAME der DNS-Name des POP-Servers angegeben wird. Das Häkchen ZERTIFIKAT WIRD „SELBST-SIGNIERT" (WURZEL) wird dieses Mal ausgeschaltet, denn wir wollen ja unsere eigene Zertifizierungsstelle das Zertifikat unterschreiben lassen. Drücken Sie auf FORTFAHREN.

3. Wählen Sie im nächsten Dialogfenster den gewünschten Aussteller. Dies sollte unsere oben erzeugte Root-Zertifizierungs-Instanz sein. Drücken Sie auf FORTFAHREN.

4. Wählen Sie den Schlüsselbund, in dem das neue Zertifikat abgespeichert werden soll.

5. Es erscheint ein Abschlussfenster, dass das neue Zertifikat erfolgreich erstellt wurde. Das Zertifikat sollte mit einem grünen Häkchen als gültig markiert sein.

Im angelegten Schlüsselbund für unsere privaten Zertifikate sollte nun drei neue Einträge, für das Zertifikat selbst und dessen Schlüssel zu finden sein. Beachten Sie, dass das Zertifikat der Zertifizierungsstelle gelb, und das „normale" Zertifikat blau dargestellt wird.

Importieren des Zertifikats

Wir haben das neue Zertifikat dieses Mal im Zertifizierungsassistenten erstellt, nicht wie in Abschnitt 9.3.3 beschrieben im Server Admin-Programm. Um das Zertifikat für den POP-Server nutzen zu können, müssen wir es erst in die Serveradministration kopieren. Hierzu sind weitere Schritte erforderlich.

1. Wählen Sie das soeben neu erzeugte (blaue) Zertifikat im Programm Schlüsselbund aus.

2. Rufen Sie den Menüpunkt ABLAGE | EXPORTIEREN... auf.

3. Wählen Sie als Dateiformat PRIVACY ENHANCED MAIL (.PEM) und ändern oder bestätigen Sie den Dateinamen.

4. Wählen Sie den soeben neu erzeugten privaten Schlüssel, der zum Zertifikat gehört, im Programm Schlüsselbund aus.

5. Rufen Sie wieder den Menüpunkt ABLAGE | EXPORTIEREN... auf.

6. Ändern oder bestätigen Sie den Dateinamen und drücken Sie auf OK.

7. Geben Sie auf Wunsch ein Kennwort ein, mit dem die Datei für den privaten Schlüssel gesichert wird. Der Schlüssel ist eine sehr sicherheitskritische Information. Je nachdem, wie Sie ihn weitergeben, ist die Vergabe eines Kennworts sinnvoll. Im Moment scheint es jedoch mit einigen Versionen von Tiger Kompatibilitätsprobleme bei der Verwendung von Schlüsseldateien zu geben, die mit einem Kennwort versehen wurden. Lassen Sie im Zweifelsfall das Kennwort leer.

8. Die Datei wird gespeichert. Das Schlüsselbund-Programm benötigt eventuell noch einmal ein Kennwort, um auf den privaten Schlüssel zugreifen zu dürfen.

An dieser Stelle gibt es ein kleineres Problem, denn das Schlüsselbund-Programm kann Schlüssel nur im Dateiformat *p12* exportieren, während Server Admin auch hier das pem-Format erwartet. Wir müssen dies über die Kommandozeile lösen. Öffnen Sie ein Terminal-Fenster und gehen Sie mit `cd` in den Ordner, in den Sie die p12-Datei gespeichert haben. Geben Sie dann den Befehl

```
openssl pkcs12 -in Mailzertifikat.p12 -nocerts -nodes -out Mailschluessel.pem
```

ein. Hierbei ist `Mailzertifikat.p12` durch den Namen der exportierten Datei und der Name `Mailschluessel.pem` durch die gewünschte Bezeichnung der Zieldatei zu ersetzen. Das Programm fragt nach dem Kennwort für die p12-Datei und erstellt daraus eine neue Datei im pem-Format. Vergewissern Sie sich im Finder, ob die Dateien im richtigen Ordner angekommen sind. Da wir immer noch im root-Account arbeiten, liegen die Dateien standardmäßig im Ordner

```
/var/root/Library/Keychains
```

Falls Sie zur Übung bereits das Spielzertifikat in Abschnitt 9.3.3 erstellt hatten und nun ein neues Zertifikat mit dem gleichen *Allgemeinen Namen* (dem DNS-Namen des jeweiligen Servers) importieren, wird Server Admin das neue Zertifikat nicht akzeptieren, da ein Dokument mit einem solchen Namen bereits vorhanden ist. In diesem Fall müssen Sie das alte Zertifikat erst löschen und die Änderung sichern, bevor Sie den Import versuchen.
Sie dürfen solche Änderungen auf keinen Fall durchführen, während Clients mit dem Server verbunden sind, da diese den Zugriff auf Open Directory verlieren würden, wenn sie zwar auf SSL konfiguriert sind, aber vorübergehend kein gültiges Zertifikat hinterlegt ist.

1. Starten Sie das Programm Server Admin und wählen Sie in der Tabelle COMPUTER & DIENSTE den gewünschten Server-Eintrag aus.
2. Wählen Sie rechts den Punkt EINSTELL. und dort ZERTIFIKATE.
3. Betätigen Sie die Schaltfläche IMPORTIEREN... rechts unten.
4. Es erscheint ein Dialogfenster zur Angabe der Dateien. Sie können die Schaltflächen mit den drei Punkten verwenden, um jeweils einen weiteren Hilfsdialog zum Suchen der Datei aufzurufen. Hierbei verhält sich das Server Admin-Programm allerdings oft fehlerhaft und zeigt nicht alle Dateien an. Geben Sie bei ZERTIFIKATSDATEI die Datei des Zertifikats an, die wir zunächst im pem-Format erstellt hatten.
5. Geben Sie bei PRIVATE SCHLÜSSELDATEI die pem-Datei an, in die wir den privaten Schlüssel umgewandelt hatten.
6. Das Feld DATEI DER ZERTIFIZIERUNGSINSTANZ kann leer bleiben. In das Feld KENNWORT FÜR PRIVATEN SCHLÜSSEL brauchen Sie nur etwas einzugeben, falls Sie beim Export des privaten Schlüssels ein Kennwort vergeben hatten. Betätigen Sie die Schaltfläche IMPORTIEREN.
7. Falls die Dateien in Ordnung sind und kein Namenskonflikt mit einem bereits bestehenden Zertifikat aufgetreten ist, wird das Zertifikat mit Name, Aussteller und Gültigkeit in die Tabelle eingetragen.

Nutzen des Zertifikats

Das private Zertifikat kann nun für Serverdienste verwendet werden. Wir verwenden es im folgenden Beispiel für den POP/IMAP-Zugang zu unserem Mailserver.

1. Wählen Sie im Programm Server Admin in der Tabelle COMPUTER & DIENSTE den Punkt MAIL aus.
2. Wählen Sie in der rechten Hälfte des Fensters den Punkt EINSTELLUNGEN und hierunter die Karteikarte ERWEITERT.

3. Schalten Sie unter dem Punkt SSL (SECURE SOCKETS LAYER) das Menü IMAP UND POP SSL je nach Wunsch auf VERWENDEN oder ERZWINGEN und wählen Sie im nebenstehenden Menü das neue Zertifikat aus.

4. Betätigen Sie die Schaltfläche SICHERN.

Nutzung auf Client-Seite

Wie erwähnt müssen alle Client-Computer im Netz darüber informiert werden, dass Sie den Server als inoffizielle Zertifizierungsstelle akzeptieren dürfen. Ist dies einmal erfolgt, so werden sie danach allen von ihm ausgestellten Zertifikaten trauen. Wir legen hierzu das Zertifikat, das uns als gültige Root-Zertifizierungs-Instanz ausweist (nicht das Zertifikat für SSL!) als Datei auf einen zentralen Fileserver oder Datenträger:

1. Starten Sie auf dem Server das Schlüsselbund-Programm und wählen Sie den Schlüsselbund X509ANCHORS aus.

2. Wählen Sie in der Liste der Zertifikate das selbst erstellte Zertifikat der Root-Zertifizierungs-Instanz (Abbildung 9.14) aus.

3. Rufen Sie den Menüpunkt ABLAGE | EXPORTIEREN auf.

4. Stellen Sie sicher, dass als Dateiformat ZERTFIKAT (.CER) eingestellt ist und geben Sie den gewünschten Ablageort für die Datei an. Drücken Sie auf SICHERN.

Auf allen Clients sind dann die folgenden Schritte vorzunehmen:

1. Melden Sie sich auf dem Client-Computer als Administrator an und stellen Sie dem Client, z.B. per File-Server, Datenträger oder E-Mail die erstellte cer-Datei zur Verfügung.

2. Doppelklicken Sie die cer-Datei im Finder.

3. Es öffnet sich das Schlüsselbund-Programm. Bestätigen Sie, dass die Datei importiert werden soll und wählen Sie als Ziel den Schlüsselbund X509ANCHORS aus (Abbildung 9.15).

Nun lassen sich auf diesem Computer alle Zertifikate, die auf dem Server ausgestellt und mit dem Root-Zertifikat signiert wurden, ohne Probleme und Warnmeldungen nutzen. Sie können beispielsweise das Programm *Mail* so umstellen, dass Ihr Mail-Account jetzt die elektronische Post per SSL vom Server abruft. Die Einstellungen sind in Mail unter MAIL | EINSTELLUNGEN... | ACCOUNTS | ERWEITERT | SSL VERWENDEN zu finden. Hätten wir das Root-CA-Zertifikat nicht auf dem Client hinterlegt, wäre beim Abrufen der E-Mail die Meldung aus Abbildung 9.16 erschienen.

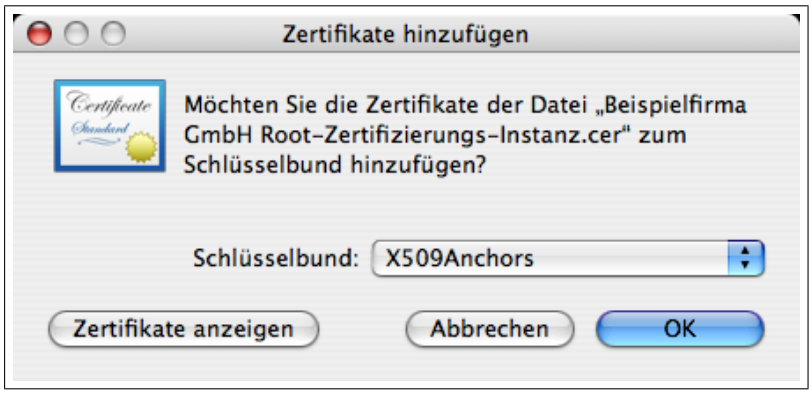

Abbildung 9.15: Auf den Client-Computern kann das private Zertifikat der selbst erzeugten Root-Zertifizierungs-Instanz per Mausklick bekannt gemacht werden.

Der SSL-Server „g4server.example.private“ konnte nicht überprüft werden.
Dieser Server hat ein Zertifikat für „g4server.example.private“ ausgestellt. Mail konnte die Identität des Servers jedoch nicht überprüfen. Fehler:
Das root-Zertifikat für diesen Server konnte nicht überprüft werden.
Möglicherweise sind Sie mit einem Computer verbunden, der vorgibt „g4server.example.private“ zu sein, und gefährden dadurch Ihre vertraulichen Informationen. Möchten Sie trotzdem fortfahren?
g4server.example.private
Ausgestellt von: Beispielfirma GmbH Root-Zertifizierungs-Instanz
Gültig bis: Montag, 30. Juni 2008 15:08 Uhr Europe/Berlin
Dieses Zertifikat wurde von einer unbekannten Instanz signiert.
Details
Zertifikat ausblenden
Abbrechen
Fortfahren

Abbildung 9.16: Ist ein Client noch nicht darüber informiert worden, dass er dem Zertifikat der privaten Zertifizierungsstelle trauen kann, werden immer noch Warnmeldungen ausgegeben.

Kapitel 10

Drucken im Netz

10.1 Verwendung von USB-Druckern an Airport-Basisstationen

Apple hat es inzwischen aufgegeben, eine Kompatibilitätsliste mit USB-Druckern zu pflegen, die mit Mac OS X und dem Drucken über die Airport-Basisstation verträglich sind. Die im Hauptbuch angegebene Internet-Adresse zum Abrufen der Verträglichkeitsliste ist nicht mehr gültig. Apple vertritt inzwischen die Meinung, dass die Druckerhersteller für die Kompatibilität verantwortlich sind. Zur Problembehebung beim Anschluss von USB-Druckern an eine Basisstation verweist Apple auf folgenden Artikel (bei Redaktionsschluss nur auf englisch verfügbar):

```
http://docs.info.apple.com/article.html?artnum=107418
```

10.2 IPP als Übertragungsprotokoll der Wahl

Inzwischen hat es sich auf allen Plattformen, egal ob Mac OS X, andere Unix-Versionen oder Windows, durchgesetzt, das im Hauptbuch erwähnte Protokoll *IPP (Internet Printing Protocol)* bevorzugt zum Netzwerktransport von Druckdaten einzusetzen. Auch in Tiger ist dies zu empfehlen, sofern für alle beteiligten Clients möglich. Da die Aktualisierung der Druckerkonfiguration von Panther auf Tiger in vielen Fällen recht holprig verläuft, bietet sich für ältere Installationen eine gute Gelegenheit, die Warteschlangen neu anzulegen und auf IPP umzustellen.

10.3 Verbesserungen im Server Admin-Programm

Das Server Admin-Programm weist in Tiger einige kleinere Verbesserungen auf:

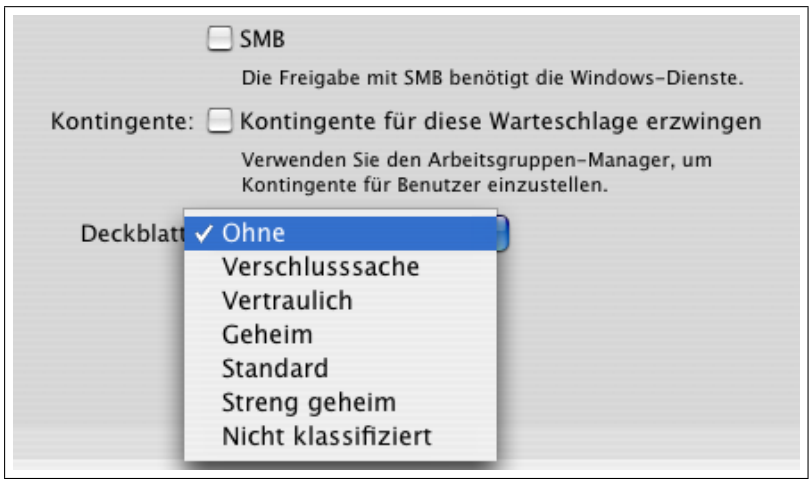

Abbildung 10.1: Der Server kann veranlasst werden, Druckjobs automatisch mit Deckblättern zu versehen, falls der druckende Client nicht von sich aus Deckblattoptionen vorgibt.

- Es ist jetzt auch von hier aus möglich, mehrere Warteschlangen zu einem *Druckerpool* zusammenzufassen.
- Im Bereich *Protokolle* steht Zugriff auf mehr von CUPS verwaltete Tätigkeitsberichte zur Verfügung.
- Bei der Einrichtung der Warteschlange kann ein Drucker so konfiguriert werden, alle Aufträge automatisch mit Deckblättern zu versehen. Apple stellt hierzu verschiedene Standardtexte zur Verfügung (Abbildung 10.1).

Die letztgenannte Option wird nur dann wirksam, wenn das druckende Client-Betriebssystem nicht schon von sich aus eine Einstellung für das Deckblatt vornimmt. Wenn Sie also von der grafischen Oberfläche eines Tiger-Systems drucken, so ist auch da eine Deckblatteinstellung vorgesehen, die als Standard auf DECKBLATT DRUCKEN: OHNE steht. Hierdurch wird das von der Server-Warteschlange vorgeschlagene Deckblatt wieder abgeschaltet und beim Ausdruck erscheint kein zusätzliches Blatt. Drucken Sie jedoch z.B. von der Unix-Kommandozeile aus auf die Warteschlange des Servers, so wird der Standardwert *auf Serverseite* aktiv und das Deckblatt wird gedruckt. Momentan erscheinen übrigens alle Deckblätter in englischer Sprache, egal auf welche Primärsprache das entsprechende Mac OS X-System konfiguriert ist.

10.4 Neue Features auf Client-Seite

Wie schon erwähnt steht auch in der Standardversion von Mac OS X eine neue Deckblattoption zur Verfügung, die im Druckermenü erscheint (Abbildung 10.2).

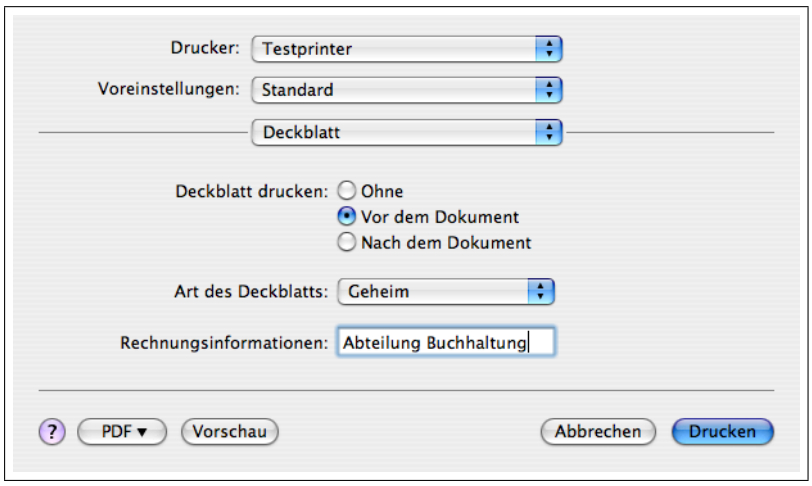

Abbildung 10.2: Client-seitig stehen mehr Deckblattoptionen zur Verfügung: Das Deckblatt kann auch nachgestellt werden und Informationen zur Abrechnung enthalten. Unabhängig von der eingestellten Sprache erscheinen die Deckblätter momentan allerdings immer auf englisch.

Das Blatt kann wahlweise vor- oder nachgestellt werden und es lässt sich ein optionaler Vermerk RECHNUNGSINFORMATIONEN auf das Blatt drucken, wer hausintern den Druckjob zahlen soll. Hiervon unabhängig wird wie bisher der Name des druckenden Benutzers erfasst, was in eine eventuell eingeschaltete Kontingentierung mit eingeht.

Die Einrichtung eines neuen Netzwerkdruckers im *Drucker-Dienstprogramm* wurde vollständig überarbeitet. Betätigen Sie die Schaltfläche HINZUFÜGEN erscheint dank Bonjour in der Rubrik STANDARD-BROWSER automatisch eine Liste der in Ihrem Teilnetz vorhandenen Mac OS X-Tiger-Druckserver, genauer gesagt deren Druckerwarteschlangen. Durch Anklicken einer der aufgelisteten Drucker werden automatisch sämtliche Einstellungen der Warteschlange vom Server übernommen und der Drucker ist sofort funktionsbereit.

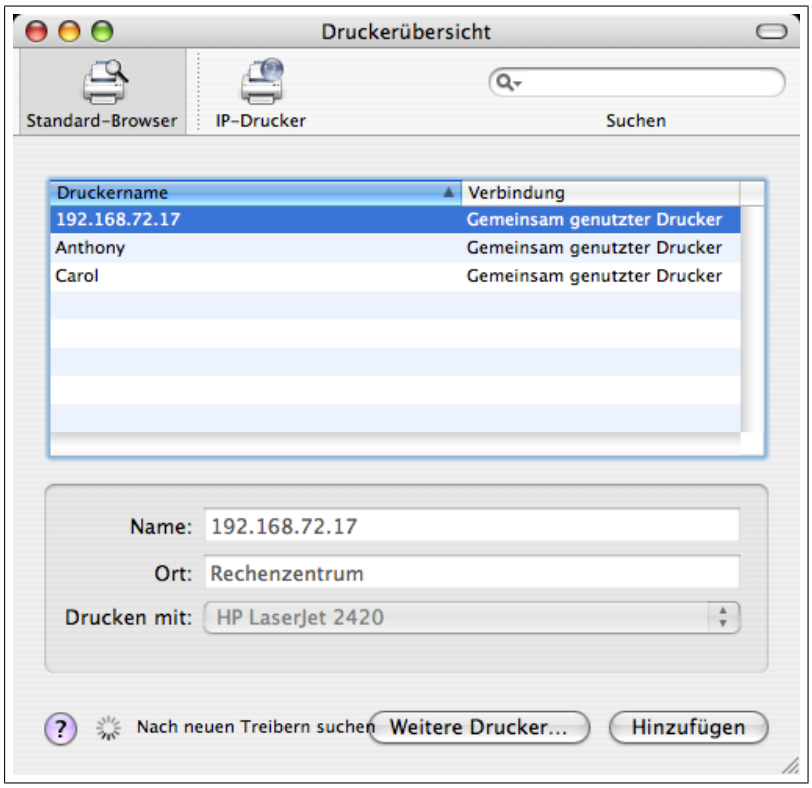

Abbildung 10.3: Dank Bonjour ist die Einrichtung eines neuen Netzwerkdruckers auf einem Klienten mit zwei Mausklicks erledigt. Voraussetzung ist, dass die Warteschlange auf einem Tiger-Server beheimatet ist.

Kapitel 11

E-Mail – die elektronische Post

11.1 Einführung

11.1.1 Korrektur

Die Internetadresse für nähere Informationen über das Postfachverwaltungssystem *Cyrus* wurde im Hauptbuch leider abgeschnitten angegeben. Die korrekte Adresse lautet

```
http://asg.web.cmu.edu/cyrus/
```

11.1.2 Überblick über die Neuerungen

Die Mail-Dienste in der Server-Version von Mac OS X Tiger wurden mit zahlreichen Neuerungen versehen. Es stehen nun einfach konfigurierbare Filtermöglichkeiten zur Verfügung, um bereits auf dem MTA unerwünschte Postsendungen, die Computerviren enthalten, als auch unerwünschte Werbung *(UCE, SPAM)* zu entfernen. Ebenso können viele Funktionen, die früher nur über die Kommandozeile oder Konfigurationsdateien abrufbar waren, jetzt komfortabler über die grafische Oberfläche von Server Admin abgerufen werden. Das Weiterleiten von E-Mail an einen MTA, der Authentifizierung verlangt (siehe Abschnitt 11.3.3 des Hauptbuchs), ist allerdings immer noch nicht vorgesehen und muss unverändert durch manuelle Anpassung der *main.cf*-Datei konfiguriert werden.

Ebenso wurde die Steuerung der Kontingentierungsmöglichkeiten stark verbessert. Das Beschränken der Postfachgröße jedes Benutzers ist noch einfacher steuerbar und Absender, die an ein überlaufendes Postfach Mails geschickt haben, können durch einstellbare Rückmeldungen über diesen Zustand informiert werden. Zudem wurde das Einrichten von *virtuellen Hosts* über die grafische Oberfläche erleichtert. Verwaltet ein MTA die Weiterleitung elektronischer Post gleich für mehrere DNS-Domänen, so lässt sich dies jetzt viel bequemer konfigurieren, als in Panther. Die

Einrichtung der neuen Funktionen wird in diesem Kapitel jeweils kurz beschrieben.

11.1.3 Aktualisierung der Mail-Dienste

Wenn Sie einen Mac OS X Server von Panther auf Tiger aktualisieren, ist in den meisten Fällen eine Übernahme der Konfiguration problemlos möglich, ohne dass zusätzliche Schritte ausgeführt werden müssen. Selbst die in Abschnitt 11.3.3 des Hauptbuchs erwähnte Warnung, dass eventuell der Inhalt der Datei

`/etc/postfix/main.cf`

neu überarbeitet werden muss, falls Sie dort Änderungen vorgenommen haben, muss im Moment nicht beachtet werden. Sind die Gliederungs- und Syntaxregeln der Datei eingehalten worden, behält das Mailsystem bei der Tiger-Aktualisierung die Einstellungen bei und es ist keine erneute Anpassung nötig.

Falls die Konfiguration Ihres Mailservers das Problem aufweisen sollte, dass zwar lokale E-Mails mit Adressen nach dem Muster

`hans` oder `hans@g4server`

korrekt zugestellt werden, die Weiterleitung von Inhaus-Mails mit den Adressen

`hans@example.private` (falls Ihre DNS-Domäne `example.private` ist)

jedoch verweigert wird, versuchen Sie zur Abhilfe, virtuelles Hosting für Ihre eigene Domäne einzuschalten. Hierzu gehen Sie nach Auswahl des Dienstes MAIL im Programm Server Admin in den Punkt EINSTELLUNGEN | ERWEITERT | HOSTING und kreuzen dort das Feld VIRTUELLES HOSTING AKTIVIEREN an. Danach fügen Sie über die Plus-Schaltfläche neben der Tabelle Ihren eigenen DNS-Domänennamen in die Tabelle ein.

11.2 Einrichtung des Mail-Servers

11.2.1 Basiseinstellungen

Öffnen Sie in Server Admin den Dienst MAIL und gehen zu EINSTELLUNGEN | ALLGEMEIN, so werden Sie neben einer starken Überarbeitung der Eingabemasken zwei neue Funktionen entdecken, die jetzt über die grafische Oberfläche verfügbar sind: Der Punkt AN „/VAR/MAIL/" ZUSTELLEN, WENN POP UND IMAP DEAKTIVIERT SIND bezieht sich auf „klassische" Art und Weise, wie E-Mail vor der Erfindung der Postfachprotokolle POP und IMAP in einem Netz an die Endbenutzer zugestellt wurde. Früher war es üblich, alle eingehenden Postsendungen auf dem Mailserver in einer Datei

```
/var/mail/<benutzername des empfängers>
```

zu speichern. Neu hinzukommende Briefe wurden hinten an diese Dateien angehängt. Damit die Post auf den Client-Computern abgerufen werden konnte, wurde der Ordner `/var/mail` per NFS in gleichnamige Ordner auf allen Klienten eingeblendet. Mail-Programme (MUAs) haben dann einfach die Dateien in diesem Ordner ausgelesen, um die Mails anzuzeigen. Unix-Programme wie PINE und ELM beherrschen diese Technik heute noch. Falls Sie diese Art der Mailzustellung bevorzugen, können Sie den entsprechenden Punkt ankreuzen und dann auf POP und IMAP verzichten.

Das zweite neue Ankreuzfeld ist AUSGEHENDE MAIL HALTEN. Es ist im Wesentlichen für vorübergehende Wartungsarbeiten am SMTP-Server gedacht. Wird das Feld angekreuzt, kann immer noch E-Mail von den Benutzern eingeliefert werden, der Server speichert jedoch die ganze Post zwischen, bis die Option wieder aufgehoben wird. Dies kann nützlich sein, um kurzzeitig die SMTP-Weiterleitung zu stoppen, beispielsweise wenn es Probleme mit der Internet-Leitung, Kommunikationsprobleme mit dem SMTP-Weiterleitungsserver oder einen „Virenverdacht“ gibt, der es erfordert, die ausgehende Mail unter Quarantäne zu stellen.

11.2.2 Kontingentierung

Falls Ihre Benutzer das Zustellungsprotokoll IMAP verwenden dürfen, werden die eingehenden E-Mails dauerhaft auf dem Server gespeichert bis sie vom jeweiligen Empfänger gelöscht werden, nicht im Mail-Programm (und damit nicht im Privatordner) des Benutzers. In diesem Fall kann es leicht passieren, dass die Nutzer zu viel Speicherplatz auf dem Mailserver verbrauchen, daher sollten Sie den Mailspeicher entsprechend kontingentieren (siehe Abschnitt 5.7.2 des Hauptbuchs). Auf der neuen Karteikarte KONTINGENTE der Maileinstellungen können Sie hierzu weitere Anpassungen vornehmen:

Der Punkt EINGEHENDE NACHRICHTEN GRÖSSER X MB ABLEHNEN erlaubt die Einstellung der maximalen E-Mail-Größe (inklusive kodiertem Anhang), die ein Benutzer empfangen darf. Ist die E-Mail größer wird sie schon beim Eingang auf dem MTA abgeblockt und der Absender mit einer Warnmeldung hierüber informiert.

Hat ein Benutzer zu viel E-Mail in seinem Server-Postfach, so kann das komplette Benutzerkonto mit dem Punkt EINGEHENDE MAIL FÜR BENUTZER BEI KONTINGENTÜBERSCHREITUNG DEAKTIVIEREN vom Empfang von E-Mail ausgeschlossen werden. Sollte dieser Fall eintreffen, wird natürlich auch hierbei der Absender durch eine entsprechende Warnmeldung informiert. Auch der Benutzer selbst kann über tägliche Warnmeldungen darüber in Kenntnis gesetzt werden, wenn er sich mit dem Mail-Speicherplatz dem kritischen Bereich nähert. Hierzu ist die Option KONTINGENTWARNUNGEN AKTIVIEREN anzukreuzen. Die gewünschte Warnmeldung, die Warnschwelle in Prozent und die Häufigkeit der Warnung in Tagen kann einzeln eingestellt werden (Abbildung 11.1).

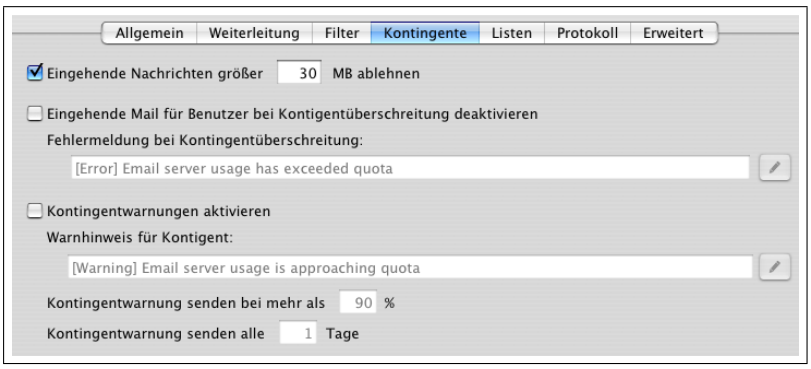

Abbildung 11.1: Tiger erlaubt es, über die grafische Oberfläche zu definieren, wie sich der Mailserver vor und nach Überschreiten von E-Mailkontingenten gegenüber dem Benutzer verhalten soll.

11.2.3 Wartungsarbeiten über Server Admin

Weitere Optionen, die früher ebenso nur über die Kommandozeile zur Verfügung standen, lassen sich im Bereich MAIL über die Rubrik WARTUNG aufrufen. Die in Panther vorhandene Rubrik ACCOUNTS ist in Tiger zum ersten Unterpunkt von WARTUNG geworden:

Über den Punkt DATENBANK können Sie schnell feststellen, wieviel Speicherplatz das Postfachsystem im Moment auf dem Server verbraucht. Außerdem ist die Reparatur der Datenbank über die grafische Oberfläche möglich. Statt das in Abschnitt 11.2.5 vorgegebene Verfahren zu benutzen, reicht es in Tiger also aus, an dieser Position die Schaltfläche REPARIEREN zu drücken.

Der verbrauchte Speicherplatz der Maildaten wird getrennt für die eigentliche DATENBANK, die nur den Index der einzelnen Mailsendungen speichert und den MAIL-SPEICHER, der die eigentlichen Inhalte der IMAP-Postfächer enthält, angegeben. Letzterer Speicher kann ab 10.4 problemlos erweitert werden, falls es Ihre Anwendungen erfordern. Sie können ein oder mehrere Festplatten hinzufügen, dort nach Wunsch Partitionen einrichten und diese Partitionen als zusätzlichen Speicherplatz für die IMAP-Postfächer konfigurieren. Die entsprechenden Partitionen werden in der Tabelle WEITERE SPEICHERORTE FÜR DEN MAIL-SPEICHER aufgelistet.

Das eigentliche Hinzufügen von neuem Speicherplatz und die Angabe des Speicherortes für Mail-Datenbank und Mail-Postfächer geschieht dagegen an einer anderen Stelle: Wählen Sie für den Dienst Mail den Punkt EINSTELLUNGEN | ERWEITERT | DATENBANK aus, so erscheinen die Eingabefelder aus Abbildung 11.2. Sie können hier die Unix-Pfade für die Ordner angeben, an denen sich die Datenbereiche befinden sollen. Mithilfe der Schaltflächen unter der Tabelle ZUSÄTZLICHE MAIL-SPEICHER können Sie zusätzliche Partitionen für die Postablagen hinzufügen oder löschen. Das Postfach welches Benutzers sich in welcher Partition befinden soll, wird über den Arbeitsgruppen-Manager (dort ACCOUNTS | BENUTZER | E-MAIL | ALTERNATIVE PARTITION VERWENDEN) eingestellt. Die Namen der Partitionen können Sie selber

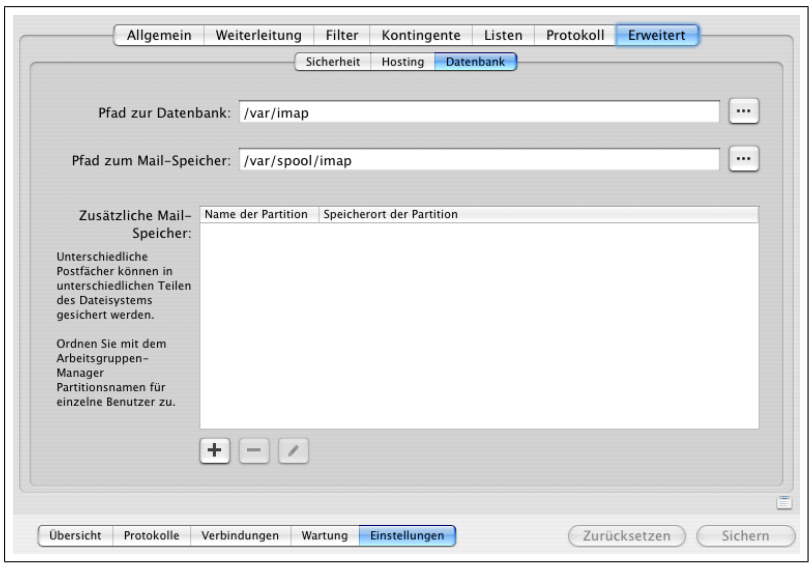

Abbildung 11.2: Die Speicherorte für die Mail-Datenbank und die IMAP-Postfächer lassen sich in Mac OS X 10.4 über die grafische Oberfläche von Server Admin konfigurieren. Die Ablage der Postfächer kann hierbei dynamisch auf mehrere Platten verteilt werden.

vergeben, sie müssen jedoch eindeutig sein.

Sie sollten die Speicherorte angeben, *bevor* Sie einen neuen Mailserver in Betrieb nehmen. Sind die Maildienste bereits in Benutzung, müssen Sie diese stoppen, die neuen Speicherorte vorgeben und hierbei *die Daten von Hand unter Beibehaltung aller Berechtigungen an den neuen Ort verschieben*. Diese Aufgabe wird nicht automatisch für Sie erledigt. Wenn Sie nur einen neuen Speicherort angeben, so erstellt das Mailsystem einen komplett neuen, leeren Arbeitsbereich am angegebenen Ort. Der alte wird beibehalten, aber nicht mehr benutzt.
Das Hinzufügen von zusätzlichem Speicher ist dagegen auch im laufenden Betrieb möglich. Aber auch dieser Speicher wird erst dann benutzt, wenn Sie bei den Benutzerkonten die jeweiligen neuen Partitionsnamen zur Mail-Ablage angeben.

Ebenfalls in der Rubrik WARTUNG finden Sie den neuen Punkt MAIL-WARTELISTE, der tabellarisch die Sendungen auflistet, die vom MTA noch nicht „nach draußen" weitergeleitet wurden. Dies kann verschiedene Gründe haben, z.B. die vorübergehende Nichterreichbarkeit des MTAs, an den die Zustellung erfolgen soll. Vielleicht haben Sie auch – wie oben beschrieben – die Zustellung angehalten, um einen Computervirus zu löschen, bevor er Ihr Netz verlässt. Mit den Knöpfen LÖSCHEN und ERNEUT VERSUCHEN können Sie bei einzelnen, noch in der Warteschlange be-

findlichen Sendungen entscheiden, was letztendlich passieren soll.

Der neue Punkt MIGRATION betrifft schließlich die Übernahme der Daten eines Mailservers von Mac OS X 10.1 oder 10.2 und wird an dieser Stelle nicht beschrieben.

11.3 Filterung von E-Mail

11.3.1 Allgemeines

Mac OS X Tiger Server kann auf Wunsch jede eingehende E-Mail daraufhin untersuchen, ob es sich möglicherweise um unerwünschte Werbemail (UCE, SPAM) handelt, bzw. ob eine Postsendung einen Computervirus enthält. Hierzu werden die freien Programme *SpamAssassin* und *ClamAV* eingesetzt. Beide Programme werden im Wesentlichen über die Karteikarte EINSTELLUNGEN | FILTER der Rubrik MAIL in Server Admin konfiguriert.

Je nachdem, in welchem Land Sie sich befinden und in welcher Rechtsbeziehung Sie zu den Nutzern Ihres Mailservers stehen, kann der Einsatz eines E-Mail-Filters illegal sein. Auch wenn Sie nur Gutes im Sinn haben, stellt dies je nach Rechtslage einen unerlaubten Eingriff in die Weiterleitung von Telekommunikationsdaten dar. Sie sollten sich bei einem Rechtsbeistand näher informieren, falls Sie diese Features einsetzen möchten.
Ebenso sollten Sie daran denken, dass bei jedem SPAM-, als auch bei jedem Virenfilter falsche Positivauskünfte vorkommen werden. Es wird also Postsendungen geben, die zu Unrecht als böswillig eingestuft werden, was weitere rechtliche Probleme und Schäden nach sich ziehen kann.

11.3.2 Ausfiltern von unerwünschter Werbepost

Das Programm SpamAssassin verwendet zur Erkennung von Werbe-Mails ein ganz anderes mathematisches Verfahren als Apple es auf Client-Seite im Programm *Mail* tut: Apple Mail verwendet ein neuronales Netz, das eine selbst anpassende *Latente Semantische Analyse (LSA)* durchführt, während SpamAssassin einen sogenannten Bayes-Filter – benannt nach dem englischen Mathematiker *Thomas Bayes* (1702–1761) – einsetzt. Beide Verfahren benötigen eine *Trainingsphase*, d.h. es müssen den Programmen positive und negative E-Mails vorgelegt werden, aus denen sie nach und nach „lernen", wie neue E-Mails zu kategorisieren sind.

Ein Bayes-Filter kann bereits nach dem Training mit circa 30 E-Mails überraschende Trefferquoten erzielen. Apple empfiehlt jedoch, dem Programm mindestens 200 unerwünschte Werbemails und 200 gültige Postsendungen vorzulegen, bevor den Analyseergebnissen vertraut wird. Falls Sie Zugriff auf eine entsprechende Anzahl von Mails haben (zum Beispiel indem Sie ein paar Tage lang von einem bereits

trainierten Apple Mail-Programm SPAM-Sendungen sammeln und diese nicht automatisch löschen lassen), können Sie das Training mit SpamAssassin selbst von Hand durchführen.

Alternativ können Sie jedoch auch ein halbautomatisches Training verwenden, für das die Mithilfe Ihrer Benutzer erforderlich ist: Sie müssen hierzu ein paar Freiwillige unter Ihren Benutzern dazu auffordern, für eine gewisse Zeit alle eingehenden E-Mails von Hand zu begutachten, ob es sich dabei um SPAM handelt, oder nicht. Die Benutzer müssen die Mails dann je nach Ergebnis an zwei hausinterne Mail-Adressen weiterleiten. Mac OS X Server lässt jede Nacht vollautomatisch das Trainingsprogramm auf diesen beiden Mail-Adressen laufen, wodurch sich die Analyseergebnisse nach und nach verbessern.

Egal für welches der beiden Trainingsverfahren Sie sich entscheiden, muss der SPAM-Filter zunächst in einer Art Probebetrieb eingeschaltet werden. Wir gehen deshalb zunächst auf die Aktivierung des Filters ein.

Einschalten und Konfigurieren des SPAM-Filters

1. Starten Sie das Programm Server Admin und verbinden Sie sich mit dem Server, der als Mailserver arbeitet.
2. Wählen Sie in der Tabelle COMPUTER & DIENSTE den Punkt MAIL aus.
3. Klicken Sie bei den Schaltflächen auf der rechten Seite unten den Punkt EINSTELLUNGEN an und gehen Sie zur Rubrik FILTER.
4. Schalten Sie den Werbefilter ein, indem Sie den Punkt E-MAIL NACH UNAUFGEFORDERTER MAIL DURCHSUCHEN ankreuzen. Es stehen sechs weitere Einstellungen zur Verfügung, die im Nachfolgenden beschrieben werden.

Die Auswahl MINIMUM FÜR JUNK-MAIL steuert, nach welcher Gewichtung der Filter den Entschluss fasst, ob es sich um eine unerwünschte Sendung handelt, oder nicht. Der Bayes-Filter berechnet intern aus jeder E-Mail eine Bewertungszahl. Ist die Zahl hoch, handelt es sich aller Wahrscheinlichkeit nach um SPAM, ist sie niedrig, dann eher nicht. Der mit dem Schieberegler einstellbare Trefferwert erlaubt Ihnen, die Schwelle einzustellen, nach der eine Postsendung als SPAM kategorisiert wird. Beachten Sie, dass bei Verwendung eines niedrigen Wertes zwar sehr viele Sendungen als SPAM eingestuft werden, gleichzeitig aber die Gefahr ansteigt, dass zulässige Mails versehentlich als unerwünscht erkannt werden.

Kein SPAM-Filter kann die E-Mails wirklich verstehen, bei der Filterbewertung handelt es sich ja um rein statistische Auswertungen von Worthäufigkeiten. Es zeigt sich in der Praxis, dass die Filterung nicht gut funktioniert, also zu Fehlern neigt, wenn Mails in einer anderen Sprache eingehen, als die, mit der die Trainingsphase durchgeführt wurde. Neben der fremden statistischen Verteilung der Worte in der anderen Sprache spielt hier auch eine Rolle, in welchem Zeichensatz die Mails kodiert sind. Beim Versand von E-Mail wird oft noch nicht das Unicode-Verfahren verwendet, sondern landestypische Zeichenkodierungen. Sie können einstellen, dass

E-Mails, die in bestimmten Sprachen oder mit bestimmten Zeichenkodierungen eingehen, generell nicht als SPAM bewertet werden.

Drücken Sie den Knopf mit dem Stiftsymbol neben dem Feld ZULÄSSIGE SPRACHEN, um die Sprachen auszuwählen, die generell nicht als SPAM einzustufen sind. Sie müssen bedenken, dass es sich auch bei der Spracherkennung um eine Schätzung handelt, die auf statistischen Methoden beruht. Auch sie kann fehlerhaft sein. Bei LOCALES werden in analoger Weise die Zeichensätze eingestellt, die von der Filterung ausgeschlossen werden sollen. Besonders im europäischen Sprachraum ist es allerdings nicht ungewöhnlich, regelmäßig elektronische Post in verschiedenen Sprachen zu erhalten. Es kann deshalb sinnvoll sein, aller hier eingetragenen Sprachen und Zeichensätze zu entfernen, damit keine Filterung anhand landessprachlicher Kriterien mehr erfolgt.

Das Klappmenü UNAUFGEFORDERTE E-MAIL WERDEN... ist die wichtigste Einstellung, die im Zusammenhang mit der SPAM-Filterung vorgenommen werden muss. Sie bestimmt, was passieren soll, wenn eine Postsendung schließlich als unerwünscht eingestuft wurde.

- Die Einstellung ABGELEHNT führt dazu, dass die Mail bereits auf dem MTA abgewiesen wird. Sie wird zusammen mit einer entsprechenden Warnmeldung an den Absender zurückgeschickt. Außerdem können Sie optional über das Ankreuzfeld BENACHRICHTIGUNG AN eine weitere E-Mail-Adresse angeben, die über diesen Vorfall informiert werden soll.

- Bei der Einstellung GELÖSCHT wird die E-Mail ohne weiteres Aufhebens gelöscht. Dies kann eine sehr gefährliche Einstellung sein, wenn der Filter nicht mit hoher Treffsicherheit arbeitet. Wie beim vorhergehenden Punkt gibt es aber auch hier die optionale Möglichkeit der BENACHRICHTIGUNG AN ein bestehendes Postfach.

- Der Punkt ZUGESTELLT veranlasst, dass die Postsendung ganz normal an den Empfänger ausgeliefert wird. Sie können jedoch zusätzlich einstellen, dass ein bestimmter Text in die Betreffzeile der Mail eingefügt wird, z.B. *[∗∗∗ WERBUNG ∗∗∗]*. Außerdem können Sie erzwingen, dass in diesem Fall die ursprüngliche Mail als Anhang eingepackt wird. Auf diese Weise bekommen Sie die Werbung nur dann zu Gesicht, wenn Sie explizit den Anhang öffnen. Dies kann besonders in dem Fall sinnvoll sein, wenn Sie auf dem empfangenden MUA einen weiteren SPAM-Filter laufen haben.

- Über die Auswahl UMGELEITET wird die E-Mail nicht an den ursprünglichen Empfänger gesandt, sondern an ein vorgegebenes Sammelpostfach, das Sie einrichten müssen.

Haben Sie die gewünschten Einstellungen vorgenommen, betätigen Sie bitte den Knopf SICHERN rechts unten im Fenster.

Ist der Filter aktiv, so werden in alle weitergeleiteten Sendungen zusätzliche Kopfzeilen mit den Schlüsselworten

```
X-Spam-Status:
X-Spam-Level:
```

eingefügt. Die Zeile hinter dem Doppelpunkt bei `X-Spam-Status` gibt die Bewertung durch den Bayes-Filter an, wobei der angegebene Wert `hits=` den Grad der Wahrscheinlichkeit angibt, dass es sich um SPAM handelt. Mail-Programme zeigen zusätzliche Kopfzeilen von Mail-Sendungen in der Regel nicht an, sie können jedoch immer sichtbar gemacht werden. In Apple Mail können Sie beispielsweise durch Auswahl des Menüpunktes DARSTELLUNG | E-MAIL | LANGE HEADER oder auch durch DARSTELLUNG | E-MAIL | REINE DATEI die verborgenen Inhalte jeder Sendung anzeigen lassen. Die Zeile, die mit `X-Spam-Level` markiert ist, ist als eine Art Balkendiagramm anzusehen, die den Grad der SPAM-Wahrscheinlichkeit noch einmal grafisch wiederholt: Je mehr Sterne desto sicherer die Beurteilung. Abbildung 11.3 zeigt eine Reihe von Werbe-Mails, die in Apple Mail empfangen und vorher von SpamAssassin korrekt mit einer Werbemarkierung versehen wurden. Für die ausgewählte Sendung wurde die Ausgabe der Kopfzeilen eingeschaltet, so dass Sie die zusätzlichen X-Spam-Angaben sehen können.

Falls Sie mehr über die interne Funktionsweise von SpamAssassin erfahren wollen, können Sie den offiziellen Webauftritt

```
http://spamassassin.apache.org/
```

der allerdings nur in englischer Sprache zur Verfügung steht, verwenden.

Manuelles Trainieren des Filters

Um den Filter zu trainieren, muss er wie im vorigen Abschnitt beschrieben eingerichtet werden. Selbstverständlich sollten Sie zunächst den Punkt UNAUFGEFORDERTE E-MAIL WERDEN: ZUGESTELLT auswählen, damit bei Falschbewertung auf keinen Fall Sendungen verloren gehen.

Legen Sie dann in einem Mail-Programm zwei Postfächer an, in die Sie sauber getrennt mindestens 200 erwünschte Mails, bzw. 200 unerwünschte Mails kopieren. Sie können hierzu jedes Mail-Programm verwenden, das die einzelnen E-Mail-Sendungen in normale Textdateien speichert, zum Beispiel Apple-Mail. Es ist wichtig, dass es sich wirklich um echte, typische E-Mail handelt, die in Ihrem Netz üblicherweise eingeht, da sonst die Lernergebnisse verfälscht werden. Sie sollten also keine Texte aus einem anderen Netz zum Anlernen des Filters verwenden.

In Apple Mail könnte Sie beispielsweise mit dem Menüpunkt POSTFACH | NEUES POSTFACH... zwei Fächer *Werbung* und *KeineWerbung* anlegen und dort mit gedrückt gehaltener alt-Taste die entsprechende Post hineinkopieren. Danach befinden sich Kopien der Sendungen sauber getrennt in den Ordnern

```
~/Library/Mail/Mailboxes/Werbung.mbox/Messages
~/Library/Mail/Mailboxes/KeineWerbung.mbox/Messages
```

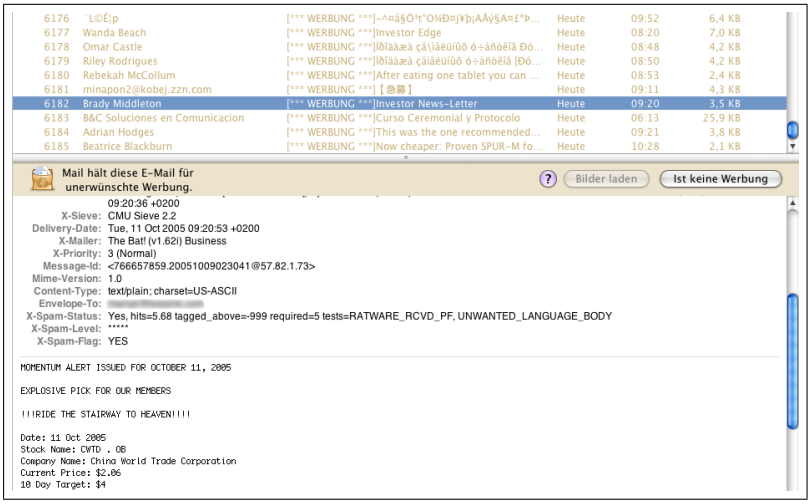
6176 L©É¦p [*** WERBUNG ***]–^¤ä§Ö³t"O¾Ð¤j¥þ¡AÁý§A¤£"Þ... Heute 09:52 6,4 KB
6177 Wanda Beach [*** WERBUNG ***]Investor Edge Heute 08:20 7,0 KB
6178 Omar Castle [*** WERBUNG ***]Ïðîàâæà çà\íåëüíûõ ó÷àñòíîâ Ðó... Heute 08:48 4,2 KB
6179 Riley Rodrigues [*** WERBUNG ***]Ïðîàâæà çàíåëüíûõ ó÷àñòíîâ [Ðó... Heute 08:50 4,2 KB
6180 Rebekah McCollum [*** WERBUNG ***]After eating one tablet you can ... Heute 08:53 2,4 KB
6181 minapon2@kobej.zzn.com [*** WERBUNG ***] [急募] Heute 09:11 4,3 KB
6182 Brady Middleton [*** WERBUNG ***]Investor News-Letter Heute 09:20 3,5 KB
6183 B&C Soluciones en Comunicacion [*** WERBUNG ***]Curso Ceremonial y Protocolo Heute 06:13 25,9 KB
6184 Adrian Hodges [*** WERBUNG ***]This was the one recommended... Heute 09:21 3,8 KB
6185 Beatrice Blackburn [*** WERBUNG ***]Now cheaper: Proven SPUR-M fo... Heute 10:28 2,1 KB
Mail hält diese E-Mail für unerwünschte Werbung.
Bilder laden
Ist keine Werbung
09:20:36 +0200
X-Sieve: CMU Sieve 2.2
Delivery-Date: Tue, 11 Oct 2005 09:20:53 +0200
X-Mailer: The Bat! (v1.62i) Business
X-Priority: 3 (Normal)
Message-Id: <766657859.20051009023041@57.82.1.73>
Mime-Version: 1.0
Content-Type: text/plain; charset=US-ASCII
Envelope-To:
X-Spam-Status: Yes, hits=5.68 tagged_above=-999 required=5 tests=RATWARE_RCVD_PF, UNWANTED_LANGUAGE_BODY
X-Spam-Level: *****
X-Spam-Flag: YES
MOMENTUM ALERT ISSUED FOR OCTOBER 11, 2005
EXPLOSIVE PICK FOR OUR MEMBERS
!!!RIDE THE STAIRWAY TO HEAVEN!!!!
Date: 11 Oct 2005
Stock Name: CWTD . OB
Company Name: China World Trade Corporation
Current Price: $2.06
10 Day Target: $4

Abbildung 11.3: Eine Reihe von unerwünschten Werbe-Mails wurde von SpamAssassin korrekt erkannt und mit einer Markierung in der Betreffzeile versehen. Zusätzlich enthält auch jede einzelne Sendung, die über den Mailserver hereinkommt, eine Bewertung, falls Sie die Filterung aktiviert haben. Schalten Sie die Anzeige der Kopfzeilen ein, so können Sie in der Zeile *X-Spam-Status* die Bewertung der Postsendung sehen. In diesem Beispiel wurde die Mail mit einem Grad von 5,68 bewertet. Da die Schwelle bei 5 *(required=)* liegt, wurde die Sendung korrekt als SPAM eingestuft und die zusätzliche Kopfzeile *X-Spam-Flag: YES* eingefügt. Hinter dem Schlüsselwort *tests=* ist eine Reihe von Schlüsselworten aufgelistet, die die Kriterien angeben, warum es sich höchstwahrscheinlich um unerwünschte Mail handelt.

wobei Sie dies am besten als Administrator durchführen, damit dieser Benutzer-Account auch Berechtigung für den Zugriff auf die Dateien hat. Nach dem Anlernen können Sie diese beiden Fächer mit POSTFACH | LÖSCHEN... wieder entfernen.

Öffnen Sie dann ein Terminal-Fenster auf dem Mailserver und geben Sie die folgenden Befehle ein:

```
sa-learn --showdots --spam ~/Library/Mail/Mailboxes/Werbung.mbox/Messages/*
```

Hiermit lernt SpamAssassin, wie üblicherweise Werbung auf Ihrem Mailserver aussieht. Die Option `-showdots` bewirkt, dass der Lernfortschritt durch eine Reihe von Punkten angezeigt wird. Das letzte Befehlszeilenargument ist der Pfad zu den entsprechenden rohen Maildateien, was Sie eventuell anpassen müssen. Der Stern als Platzhalter bewirkt, dass nicht nur die im Ordner enthaltenen Dateien, sondern auch alle Unterordner durchsucht werden, was wichtig sein kann, wenn Sie nicht Apple Mail, sondern ein Mail-Programm verwenden, das die Post in einer anderen Art und Weise ablegt. Die Verarbeitung der Daten wird einige Minuten in Anspruch nehmen. Mit dem Befehl

```
sa-learn --showdots --ham ~/Library/Mail/Mailboxes/KeineWerbung.mbox/Messages/*
```

wird dem Filter die „normale" E-Mail zur Begutachtung vorgelegt. Beachten Sie, dass hier die Option `-ham` lautet. Falls Sie versehentlich Mails falsch kategorisiert haben, ist dies kein größeres Problem: SpamAssassin identifiziert jede einzelne Postsendung und kann sie wiedererkennen. Wenn Sie mit den falschen eingeordneten Mails die Lernphase später mit der richtigen Kategorisierung wiederholen, wird das Programm die Bewertung anpassen und damit die Fehler automatisch korrigieren.

Halbautomatisches Trainieren des Filters

Wie bereits erwähnt, kann der Filter auch nach und nach angelernt werden, indem Sie Benutzer veranlassen, typische Mails an zwei bestimmte Mail-Adressen in Ihrem Hause weiterzuleiten.

1. Starten Sie das Programm Arbeitsgruppen-Manager für den Server, auf dem die Mail-Dienste laufen.
2. Legen Sie ein neues Benutzerkonto mit dem Kurznamen *junkmail* an. Sie dürfen diesen Namen nicht abändern. Es ist nicht nötig, dass Sie den Account im netzweiten Verzeichnisknoten anlegen, der Benutzer muss nur lokal auf dem Server bekannt sein. Wählen Sie also vorher am besten den Punkt LOKAL im Menü neben dem kleinen Globussymbol aus.
3. Speichern Sie das neue Benutzerkonto durch Betätigen der Schaltfläche SICHERN, gehen Sie dann zur Rubrik E-MAIL und schalten den Auswahlknopf auf E-MAIL: AKTIVIERT, so dass für diesen Account ein Postfach eingerichtet wird.

4. Wiederholen Sie die letzten Punkte, indem Sie noch ein zweites Benutzerkonto mit dem Kurznamen *notjunkmail* anlegen. Auch dieser Name darf nicht abgeändert werden.

Veranlassen Sie nun eine Reihe von Benutzern in Ihrem Netz, ein paar Tage lang alle E-Mails, die sie erhalten,

- an die Mailadresse *junkmail* in Ihrem Netz weiterzuleiten, falls es sich um Werbung handelt,
- an die Mailadresse *notjunkmail* weiterzuleiten, falls es sich nicht um Werbung handelt.

SpamAssassin wertet die Postfächer dieser beiden Benutzer jede Nacht um 1 Uhr aus, falls sie existieren, und führt damit eine Lernphase durch, wodurch sich die Bewertungsergebnisse nach und nach verbessern. Nach einer gewissen Laufzeit können Sie die beiden Benutzerkonten und ihre Postfächer wieder löschen.

11.3.3 Ausfiltern von Computerviren

Eng mit der Filterung unerwünschter E-Mail verbunden ist das Filtern von Viren und ähnlichen Schadprogrammen wie z.B. Trojanischen Pferden. Diese Funktionen werden in der unteren Hälfte des Fensters MAIL | EINSTELLUNGEN | FILTER in Server Admin konfiguriert (Abbildung 11.4).

Ein Ankreuzen des Feldes E-MAIL NACH VIREN DURCHSUCHEN reicht aus, um das Programm ClamAV zu aktivieren. Wie jedes Antivirenprogramm ist auch diese Anwendung auf eine stets aktuelle Datenbank bekannter Viren angewiesen. Die Option DATENBANK FÜR JUNK-MAIL UND VIREN X MAL AM TAG AKTUALISIEREN erlaubt die Einstellung, ob und wie oft pro Tag diesen Datenbank neu über das Internet abgefragt werden soll. Besonders vorsichtige Administratoren stellen hier mehrere Prüfungen pro Tag ein, wenn die Internet-Bandbreite ausreicht. Die bei Tiger mitgelieferte Antivirus-Datenbank bleibt auf dem Stand von März 2005, falls Sie diese nicht aktualisieren sollten.

Entscheidend für die Aktivität des Virenscanners sind die Einstellungen, die sich unterhalb von E-MAIL NACH VIREN DURCHSUCHEN befinden. Das Klappmenü INFIZIERTE E-MAILS WERDEN: definiert die Aktion, die der Scanner veranlassen soll, falls in einer E-Mail ein Virus oder ein ähnliches Schadprogramm erkannt wurde:

- ABGELEHNT bewirkt, dass die E-Mail vom MTA erst gar nicht angenommen wird. Der Absender erhält eine entsprechend Nichtannahmenachricht.
- GELÖSCHT entfernt die Sendung kommentarlos.
- ISOLIERT führt dazu, dass die Mail an ein spezielles Postfach, das Sie angeben müssen, weitergeleitet wird. Der Virus wird hierbei nicht entfernt. Der Benutzer, der dieses Isolierungspostfach später eventuell öffnet, sollte also genau wissen, was er tut.

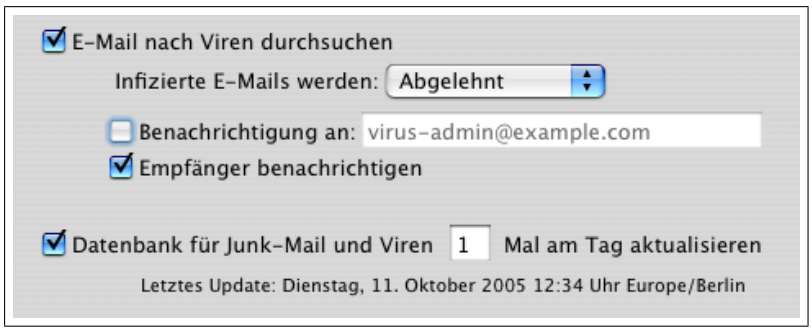
E-Mail nach Viren durchsuchen
Infizierte E-Mails werden: Abgelehnt
Benachrichtigung an: virus-admin@example.com
Empfänger benachrichtigen
Datenbank für Junk-Mail und Viren 1 Mal am Tag aktualisieren
Letztes Update: Dienstag, 11. Oktober 2005 12:34 Uhr Europe/Berlin

Abbildung 11.4: Der Virenscanner für die Maildienste wird mit wenigen Handgriffen aktiviert.

In den ersten beiden Fällen kann auch eine andere E-Mail-Adresse mit BENACHRICHTIGUNG AN und auch der ursprüngliche Empfänger der E-Mail mit EMPFÄNGER BENACHRICHTIGEN über die Situation informiert werden. Letzteres ist sinnvoll, besonders dann, wenn es sich nicht um böswillige E-Mail gehandelt hat, sondern wenn z.B. ein Geschäftspartner Ihnen unabsichtlich einen infizierten Anhang zugesandt hat. Abbildung 11.5 zeigt, wie eine solche Information aussieht. Der Typ des Virus wird angezeigt und es wird falls möglich auch versucht, die wahre Einlieferungsstelle der Postsendung zu ermitteln. Dies ist eine interessante Angabe, denn die meisten Viren werden mit gefälschten Absenderadressen versandt.

Falls Sie detaillierte Informationen zum technischen Hintergrund von ClamAV oder von Viren und deren Benennung benötigen, können Sie die Herstellerdokumentation unter der Internetadresse

```
http://www.clamav.net/
```

abrufen. Informationen über die Tätigkeiten des Filters und Hinweise auf gefundene Viren können Sie als Administrator in Server Admin bekommen, indem Sie unter MAIL | PROTOKOLLE die neuen Klappmenüpunkte SUCHE NACH UNAUFGEFORDERTER MAIL/VIREN, VIRUS und UPDATE DER VIRUS-DATENBANK aufrufen.

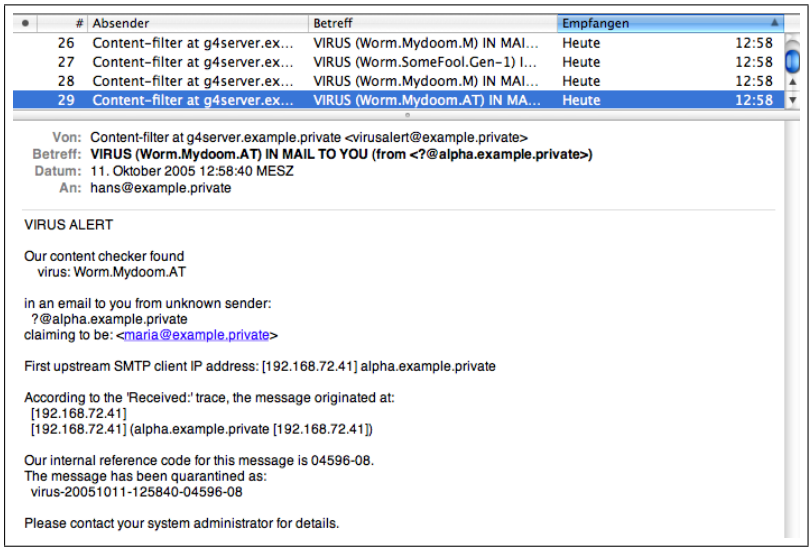
#
Absender
Betreff
Empfangen
26 Content-filter at g4server.ex... VIRUS (Worm.Mydoom.M) IN MAI... Heute 12:58
27 Content-filter at g4server.ex... VIRUS (Worm.SomeFool.Gen-1) I... Heute 12:58
28 Content-filter at g4server.ex... VIRUS (Worm.Mydoom.M) IN MAI... Heute 12:58
29 Content-filter at g4server.ex... VIRUS (Worm.Mydoom.AT) IN MA... Heute 12:58
Von: Content-filter at g4server.example.private <virusalert@example.private>
Betreff: VIRUS (Worm.Mydoom.AT) IN MAIL TO YOU (from <?@alpha.example.private>)
Datum: 11. Oktober 2005 12:58:40 MESZ
An: hans@example.private
VIRUS ALERT
Our content checker found
virus: Worm.Mydoom.AT
in an email to you from unknown sender:
?@alpha.example.private
claiming to be: <maria@example.private>
First upstream SMTP client IP address: [192.168.72.41] alpha.example.private
According to the 'Received:' trace, the message originated at:
[192.168.72.41]
[192.168.72.41] (alpha.example.private [192.168.72.41])
Our internal reference code for this message is 04596-08.
The message has been quarantined as:
virus-20051011-125840-04596-08
Please contact your system administrator for details.

Abbildung 11.5: Ist die Option eingeschaltet, den Empfänger bei Eingang einer von Viren befallenen E-Mail zu benachrichtigen, wird die Originalmail durch eine Nachricht in dieser Form ersetzt. Die Art des Virus und die wahrscheinliche, wahre Herkunftsadresse — nicht die oft gefälschte Absenderadresse — werden angezeigt.

Kapitel 12

Web-Dienste

Bezüglich der eigentlichen Web-Server-Funktionen hat sich in Mac OS X Tiger nichts geändert. Sowohl in der Serverversion als auch in der Standardfassung ist die eingesetzte Software wie bisher *Apache* Release 1.3. Neu hinzugefügt in der Serverversion wurde neben einer uneingeschränkten Laufzeitlizenz für Apples Web-Applikationsserver *WebObjects*, ein RSS-orientierter Weblog-Dienst und ein Instant-Messaging-Service, die wir in diesem Kapitel kurz beschreiben. Überarbeitet wurde zudem der QuickTime Streaming Server und seine Hilfsprogramme. Von Drittanbieterseite müssen wir außerdem auf Änderungen bezüglich der Proxy-Cache-Software DansGuardian und Squid eingehen, die im Hauptbuch zum Einsatz für professionelle Zwecke empfohlen wurden.

12.1 Nutzung eines Proxy-Cache-Servers

12.1.1 Arbeiten mit automatischer PAC-Konfiguration

Einrichten von Mac OS X-Klienten

Apple hat im Programm System-Einstellungen die Möglichkeiten zur automatischen Konfiguration auf einen Proxy-Cache-Server in der Benutzerführung überarbeitet: Im Punkt NETZWERK | PROXIES gibt ein neues Klappmenü PROXIES KONFIGURIEREN, das auf den Punkt PAC-DATEI VERWENDEN voreingestellt ist. Es braucht nur noch ein Pfad zu einer PAC-Datei oder die URL-Adresse für eine solche Datei angegeben zu werden (Abbildung 12.1). Die aus Panther bekannten Optionen stehen aber auch in der alten Form noch zur Verfügung, wenn das Menü auf den Punkt MANUELL umgeschaltet wird.

Leider funktioniert die Verwendung von PAC-Dateien im Zusammenhang mit der Tiger-Version von Safari bis einschließlich Mac OS X 10.4.2 nur mangelhaft: Egal ob der neue Menüpunkt oder die bisherige alte Einstellung AUTOM. PROXY-KONFIGURATION verwendet wird, stürzt Safari regelmäßig nach kurzer Benutzungszeit ab,

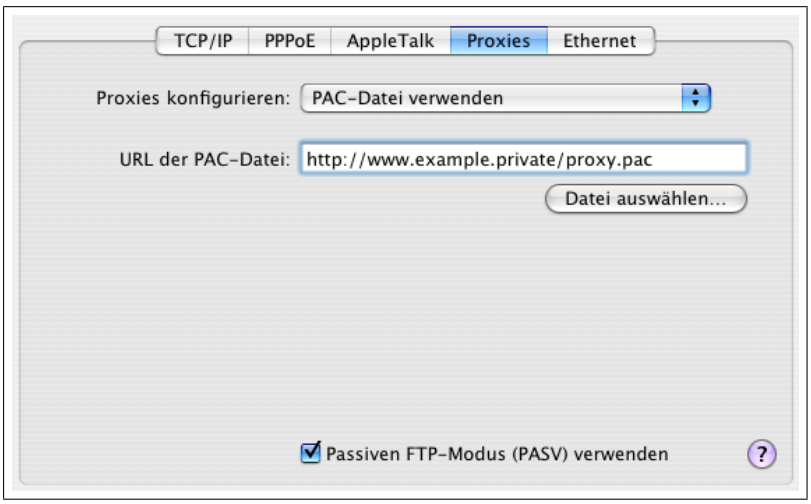

Abbildung 12.1: Die Einstellmöglichkeiten zur automatischen Proxy-Konfiguration wurden in Tiger überarbeitet und noch einfacher gestaltet. Eigentlich eine gute Sache, doch führt die Verwendung von PAC-Dateien zu einem sehr instabilen Betrieb von Safari. Das Umstellen auf manuelle Konfiguration behebt das Problem, bis Apple eine funktionsfähige Lösung bietet.

was die Verwendung von PAC-Dateien in der Praxis verbietet. Bis Apple den Fehler behebt, ist deshalb zur manuellen Konfiguration von Proxy-Servern zu raten. Dies funktioniert einwandfrei.

Hinweise zur Geschwindigkeitsoptimierung auf den Clients

In Kapitel 12.2.3 des Hauptbuchs werden zwei mögliche Musterlösungen für PAC-Dateien zur automatischen Konfiguration eines HTTP-Proxy-Servers vorgestellt. Die in Listing 12.2 wiedergegebene Lösung ist zwar wesentlich eleganter programmiert und entspricht auch den Vorschlägen, die von Netscape – dem ursprünglichen Erfinder der PAC-Konfiguration – gegeben werden, stellt aber nicht die schnellste Lösung dar: Leider gibt es viele Browser und Betriebssysteme, die die nötigen Adressprüfungen und DNS-Anfragen nur sehr ineffizient ausführen. Je nach Ihrer Netzumgebung kann es also sein, dass die „gut programmierte" Konfigurationsfunktion wesentlich langsamer interpretiert wird, als die Einfachlösung in Listing 12.1.

Sollten Sie also bei Verwendung von Listing 12.2 Geschwindigkeitsbußen beim Laden von Webseiten feststellen, so ist zu empfehlen, auf die einfachere Lösung aus Listing 12.1 auszuweichen.

12.1.2 Alternative Lösungen für Proxy und Inhaltsfilterung

Das im Hauptbuch empfohlene, kostenlose und quelloffene Programm *Squid* sowie dessen Partner *DansGuardian* leisten auch in Tiger gute Dienste. Die Mac OS X-Portierung der Programme hat inzwischen *Dave Lopata* übernommen, deshalb hat sich auch die Adresse zum Herunterladen der Software geändert. Sie lautet jetzt etwas sperrig

```
http://mambo.lopata.net/component/option,com_docman/task,cat_view/gid,14/Itemid,29/
```

Die Änderungen, die sich bei der Installation der neu zusammengestellten Software ergeben, stellen wir im Folgenden kurz vor.

Neuinstallation der Software

Das Paket aus Dansguardian, Squid und zwei neuen Hilfsprogrammen zur Konfiguration wird in Form einer Unix-tar-gz-Datei *DGComplete* angeboten. Nach dem Auspacken erhalten Sie die Software installationsfertig als Mac OS X-Paketdateien. Bei Redaktionsschluss waren Squid Version 2.5 Stable 10 und DansGuardian Version 2.8.0.4 Bestandteil des Pakets. Kopieren Sie die Software auf ein Tiger-System, das als Proxy-Server dienen soll, und starten Sie als Administrator durch Doppelklick auf *dgcomplete.pkg* die Installation. Es reicht aus, wenn Sie eine EINFACHE INSTALLATION auswählen. Als Zielordner sollten Sie den Programmeordner oder einen Unterordner davon auswählen.

Nach Abschluss der Installation finden Sie ein Programm *DG Console* im Zielordner. Es handelt sich um eine für Mac OS X entwickelte grafische Benutzeroberfläche, um DansGuardian und Squid zu konfigurieren, ohne dass Sie die Kommandozeile bemühen müssen. Das Programm ist sogar zu großen Teilen ins Deutsche übersetzt. Die im Hauptbuch beschriebenen technischen Kenntnisse über die Funktionsweise und Konfiguration der beiden Programme sind allerdings trotzdem unabdingbar. Da das Programm sowohl von der Gestaltung als auch von der Benutzerführung nicht besonders „Mac-like“ ist und auch die handprogrammierte Frage nach dem Administrationskennwort unter sicherheitstechnischen Aspekten nicht besonders überzeugt, werden wir das Programm im Folgenden allerdings nicht beschreiben, sondern wie bisher zur Arbeit direkt an den Konfigurationsdateien raten. Bestenfalls zum Starten und Stoppen der Dienste lässt sich die DG Console brauchbar einsetzen.

Die eigentlichen Hintergrundprogramme, die die Arbeit erledigen, befinden sich nicht mehr wie früher unter */usr/local*, sondern nun unter

```
/opt/squid
/opt/dansguardian
```

Auf einem Tiger-System werden automatisch Startdateien für das neue launchd-Verfahren (Abschnitt 2.1) am korrekten Ort, nämlich

```
/Library/LaunchDaemons
```

erzeugt, so dass die Dienste beim Systemstart automatisch mitgestartet werden.

Konfiguration von Squid

Bevor Sie Squid zum ersten Mal einsetzen, müssen Sie die Konfigurationsdatei an Ihren Server anpassen, so wie in Abschnitt 12.3.2 des Hauptbuchs beschrieben. Es ergeben sich zur hier vorgestellten Version die folgenden Änderungen:

Die Änderung der Konfigurationsdatei erfolgt jetzt an einem anderen Ort:

```
sudo pico /opt/squid/etc/squid.conf
```

Das Starten von Squid geschieht nun mit dem Befehl

```
sudo launchctl load /Library/LaunchDaemons/org.squid-cache.squid.plist
```

Beendet wird der Dienst durch Eingabe von

```
sudo launchctl unload /Library/LaunchDaemons/org.squid-cache.squid.plist
```

12.1.3 Konfiguration von DansGuardian

Das DansGuardian-Team ist momentan dabei, die Dokumentation und Wartung des Programms auf *SourceForge* umzustellen, den weltweiten Dienst zur Pflege und Weiterentwicklung offener Software. Sie können verschiedene Versionen der Dokumentation mit Benutzerführung in verschiedenen Sprachen unter der neuen Adresse

```
http://sourceforge.net/docman/index.php?group_id=131757
```

abrufen. Die zentrale Konfigurationsdatei befindet sich nun unter

```
/opt/dansguardian/etc/dansguardian.conf
```

In der Konfigurationsdatei befindet sich eine neue interessante Einstellung, nämlich ein Verweis auf einen Schablonendatei zur Ausblendung einer Webseite in einer übersetzten Version. Möchten Sie die Ablehnungsmeldung auf Deutsch erhalten, so suchen Sie bitte die Zeile mit der Markierung `language` und stellen diese auf

```
language = 'german2'
```

Abbildung 12.2: DansGuardian wird in der neuen Version auch mit Fehlermeldungsschablonen in deutscher Sprache geliefert.

um. Danach erscheinen die Ablehnungsmeldungen in deutscher Sprache, wie in Abbildung 12.2.

Eine Schwarze Liste mit Internet-Adressen lässt sich wie bisher von *urlblacklist.com* herunterladen. Wenn Sie sich mit `cd` im Ordner befinden, in dem der Ordner mit den ausgepackten Blacklists liegt, können Sie diese mit dem Befehl

```
sudo cp -R blacklists /opt/dansguardian/etc
```

an ihren Einsatzort kopieren. In der Datei

```
/opt/dansguardian/etc/bannedsitelist
```

wäre dann gemäß den Anweisungen in Kapitel 12.3.3 des Hauptbuchs zum Beispiel die Konfigurationszeile

```
.Include</opt/dansguardian/etc/blacklists/ads/domains>
```

am Ende einzufügen. Starten und Stoppen des Programms geschieht über

```
sudo launchctl load /Library/LaunchDaemons/org.dansguardian.dansguardian.plist
sudo launchctl unload /Library/LaunchDaemons/org.dansguardian.dansguardian.plist
```

12.2 Apples Erweiterungsmodule zu Apache

Bei den von Apple mitgelieferten Modulen des Webservers ist zu beachten, dass ab 10.4 das im Hauptbuch erläuterte Modul *mod_sherlock_apple* nicht mehr mitgeliefert wird. Die Technologie *Sherlock* wurde von Apple aufgegeben und durch Spotlight ersetzt. Dementsprechend gibt es ein neues Modul mit der Bezeichnung *mod_spotlight_apple*.

Um dieses Modul zu nutzen, müssen Sie Spotlight zumindest für den Datenbereich, in dem die HTML-Dateien Ihres Webservers liegen, einschalten. Wie bereits erwähnt ist Spotlight aus gutem Grund in einer Installation von Mac OS X Server deaktiviert. Wenn Sie Spotlight auch nur teilweise einschalten, kann das einige Performance-Probleme nach sich ziehen, so dass Sie diese Funktion nur dann nutzen sollten, wenn es unbedingt nötig ist, und der Server ausschließlich als Web-Server arbeitet.

Um Spotlight auf den Web-Speicherbereich anzusetzen, muss zunächst das physische Volume, auf dem die Web-Dokumente liegen, für die Benutzung von Spotlight freigeschaltet werden. Dies geschieht durch Eingabe des Befehls

```
sudo mdutil -i on /
```

Hierbei sind wir davon ausgegangen, dass der Web-Speicherbereich sich an seinem Standardort, also auf dem Start-Volume / im Ordner

```
/Library/WebServer/Documents
```

befindet. Sollte Sie dies so umkonfiguriert haben, dass ein anderes Volume oder mehrere Volumes benutzt werden, so müssen Sie auch diese mit *mdutil* freischalten und die Pfadangabe / entsprechend ersetzen.

Die eigentliche Indexerstellung für Spotlight wird manuell mit dem Befehl *mdimport* ausgelöst. Legen wir wieder den Standardablagepfad zugrunde, so lautet der Aufruf

```
sudo mdimport -f /Library/WebServer/Documents
```

bei anderen Ordnern ist die Pfadangabe wieder entsprechend anzupassen, bzw. mehrere Aufrufe einzugeben. Die Option `-f` ist wichtig, um zu erzwingen, dass Spotlight wirklich alle Dateien im Webordner indexiert. Intern hat Spotlight nämlich bestimmte Namensregeln, die automatisch Dateien und Ordner mit bestimmten Namen ausschließen würden. Beachten Sie allerdings, dass auch bei diesem manuellen Aufruf die gleichen Beschränkungen für Dateitypen gelten, wie im herkömmlichen Spotlight-Betrieb: Proprietäre Dateiformate, für die der Hersteller der zugehörigen Programme keine Spotlight-Import-Unterstützung anbietet, bleiben auch in diesem Fall aus dem Index ausgeschlossen. Apple unterstützt jedoch die meisten gängigen Dateiformate von Hause aus.

1. Starten Sie danach Server Admin und verbinden Sie sich mit dem Server, auf dem die Web-Dienste laufen.

2. Wählen Sie in der Tabelle COMPUTER & DIENSTE den Punkt WEB aus.
3. Gehen Sie im rechten Teil des Fensters zur Rubrik EINSTELLUNGEN und wählen dort den Punkt MODULE aus.
4. Suchen Sie das Modul APPLE_SPOTLIGHT_MODULE und kreuzen Sie das Feld AKTIVIERT an.
5. Speichern Sie die Änderung durch Druck auf die Schaltfläche SICHERN ab.

Danach können Nutzer, die auf Ihren Webserver zugreifen, Web-Dokumente nach Inhalt durchsuchen lassen. Hierzu ist es notwendig, dass eine spezielle HTML-Datei mit dem Namen *template.spotlight* im Stammordner der entsprechenden Website gespeichert ist. Apple stellt eine solche Datei als Vorlage bereits unter

```
/Library/WebServer/Documents/template.spotlight
```

zur Verfügung. Sie können die Datei nach eigenen Wünschen anpassen. Wenn Ihr Webserver mehrere virtuelle Hosts beherbergt, müssen Sie die Datei jeweils in die Stammordner der entsprechenden Sites kopieren. Die HTML-Datei besteht im Kern aus einem HTML-Formular nach dem Muster

```
<FORM ACTION=".spotlight" METHOD="post">
```

dem eine spezielle Ergebnismarkierung

```
<SPOTLIGHTOUT>
```

folgt. Um das Ganze schließlich auf Client-Seite zu nutzen, müssen Sie einen Web-Link der Form

```
http://www.example.private/.spotlight
```

aufrufen. Abbildung 12.3 zeigt, wie eine typische Suchabfrage mit der von Apple vorgegebenen Schablone aussieht. Es ist darauf hinzuweisen, dass Spotlight – wie sonst auch – die Dokumententreffer nach Güte sortiert. Es ist jedoch nicht möglich, eine „Rang"-Angabe in Form von horizontalen Balken ausgegeben zu bekommen.

12.3 Der Weblog-Dienst Blojsom

Unter dem plakativen Titel *Dienste für die Zusammenarbeit* liefert Apple die Serverversion von Mac OS X Tiger unter anderem mit dem Weblog-Dienst *Blojsom* aus. Blojsom wird wie *blossom*, dem englischen Wort für „Blüte" ausgesprochen. Der Dienst hilft dabei, die neumodische Tätigkeit des *Bloggens* – dem interaktiven Veröffentlichen von Tagebüchern im Internet mit der Möglichkeit der Zusammenfassung und Kommentierung – durch eine komfortable Umgebung zu unterstützen. In einem Firmennetz können Blogs beispielsweise als virtuelles Schwarzes Brett oder als Hilfsmittel zur technischen Dokumentation und Diskussion eingesetzt werden.

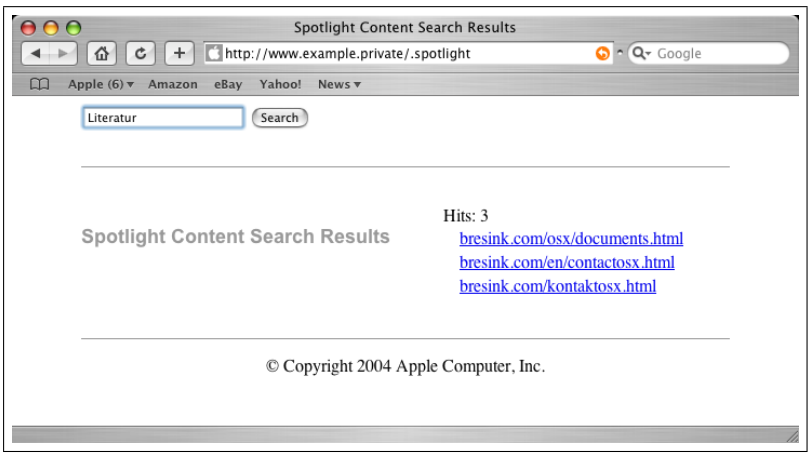

Abbildung 12.3: Spotlight kann in Tiger auch zur Suche nach veröffentlichten Web-Dokumenten genutzt werden. Hierzu ist es nötig, die Sites von Hand mit einem Spotlight-Index zu versehen und Apples neues Spotlight-Modul für Apache zu aktivieren.

12.3.1 Einrichten des Weblog-Dienstes

Die Dateien von Blojsom befinden sich im Ordner

```
/Library/Tomcat/blojsom_root
```

Aus Sicht des Administrators ist das Einrichten von Blojsom ein Kinderspiel. Es muss im Prinzip nur ein Häkchen im Programm Server Admin gesetzt werden:

1. Starten Sie Server Admin und verbinden Sie sich mit dem Server, auf dem die Weblog-Dienste eingerichtet werden sollen. Auf diesem Server müssen bereits die Web-Dienste aktiviert sein.
2. Wählen Sie in der Tabelle COMPUTER & DIENSTE den Punkt WEB aus.
3. Gehen Sie in der rechten Seite des Fensters zum Punkt EINSTELLUNGEN und wählen dort die Rubrik WEBLOGS aus.
4. Setzen Sie das Häkchen bei WEBLOGS AKTIVIEREN.

Mit den weiteren drei Feldern (Abbildung 12.4) können Sie zusätzliche Einstellungen festlegen. Das Klappmenü STANDARDTHEMA wählt einen bestimmten Darstellungsstil aus, mit dem Weblogs standardmäßig angezeigt werden sollen. Technisch stecken dahinter normale CSS-Stylesheets, die im Blojsom-Ordner (siehe unten) abgelegt sind.

Der Ort, an dem eigentlichen Blogs gespeichert werden, wird mit dem Feld WEBLOG-ORDNER vorgegeben. Apples Vorschlag folgt den üblichen Richtlinien für Mac OS X-Anwendungen und lautet

Abbildung 12.4: Der Administrator hat beim Einrichten des Weblog-Dienstes wenig zu tun. Nur ein paar Einstellungen sind zur Inbetriebnahme nötig. Die Organisation des Dienstes wird von den Weblog-Teilnehmern selber durchgeführt.

```
/Library/Application Support/Weblogs
```

es steht Ihnen aber frei, aus organisatorischen Gründen einen anderen Ordner anzugeben. Beachten Sie, dass Sie den Ordner einstellen sollten, *bevor* Sie den Weblog-Dienst in Betrieb nehmen, da bereits angelegte Blogs nicht an den neuen Ort umkopiert werden. Im Feld E-MAIL-DOMAIN sollten Sie den DNS-Domänennamen der Domäne eintragen, unter der die Blog-Benutzer üblicherweise elektronische Post empfangen. Diese Einstellung wird von Blojsom benutzt, um in der Benutzerführung jeweils gültige E-Mail-Adressen zur Kontaktaufnahme mit den Blog-Teilnehmern angeben zu können.

Aus Sicht des Verwalters ist dies fast alles, was zu tun ist. Alle anderen Aufgaben werden direkt von den Blog-Teilnehmern selber erledigt, was wir im Folgenden kurz beschreiben. Als Administrator sollten Sie nur darauf achten, dass der oben erwähnte Blog-Ordner regelmäßig in einer Datensicherung gesichert wird. Wichtig in diesem Zusammenhang sind auch die folgenden Hinweise:

Die Stylesheets im CSS-Format befinden sich in den Ordnern

```
/Library/Tomcat/blojsom_root/webapps/ROOT/blojsom_resources/stylesheets
/Library/Tomcat/blojsom_root/webapps/ROOT/blojsom_resources/includes
```

Die Protokolle über den Betrieb des Weblog-Dienstes befinden sich im Ordner

```
/Library/Tomcat/blojsom_root/logs
```

Es ist ein Hauptprotokoll und jeweils ein Protokoll für jeden Betriebstag vorhanden. Interessanterweise können diese Berichte nicht über Server Admin angezeigt werden.

Die persönlichen Einstellungen, die jeder Weblog-Teilnehmer für seine eigenen Blogs vornehmen kann, werden in Unterordnern von

```
/Library/Tomcat/blojsom_root/webapps/ROOT/WEB-INF
```

gespeichert, wobei die Unterordner den Kurznamen des jeweiligen Benutzers tragen. Sollten Sie nähere Informationen über den technischen Hintergrund von Blojsom benötigen, so können Sie die offiziellen Webseiten des Programms unter

```
http://wiki.blojsom.com/wiki/
```

aufrufen.

12.3.2 Aufruf der Weblog-Funktion

Um auf ein Weblog zuzugreifen, starten Sie einen Web-Browser und rufen die Adresse

```
http://www.example.private/weblog/
```

auf. Hierbei ist *www.example.private* natürlich durch den DNS-Namen des Servers zu ersetzen, auf dem der Weblog-Dienst läuft. Falls Sie für Ihren Web-Server ein SSL-Zertifikat eingerichtet haben, können Sie statt des Protokolls `http:` alternativ auch das Protokoll `https:` verwenden, wodurch die Daten bei der Übertragung verschlüsselt werden. Dies ist besonders dann wichtig, wenn die Weblogs dazu benutzt werden, um möglicherweise vertrauliche Firmeninformationen zu diskutieren. Da sich die Benutzer am Weblog-Dienst anmelden müssen, um Beiträge zu erstellen, betrifft dies natürlich auch die Übertragung der Kennworte.

Wenn Sie direkt auf das Blog eines bestimmten Benutzers zugreifen möchten, können Sie an die oben genannte Adresse auch den Kurznamen des Benutzers anhängen. Für den Benutzer mit dem Account `hans` also zum Beispiel

```
http://www.example.private/weblog/hans/
```

12.3.3 Terminologie und Funktionen des Bloggens

Bei der Arbeit mit Weblogs hat sich eine eigene Terminologie herausgebildet, um bestimmte Grundfunktionen zu beschreiben. Ein *Weblog* oder kurz *Blog* ist ein elektronisch geführtes Dokument, das in einem Netzwerk abgerufen werden kann und wie ein Tagebuch organisiert ist. Ein Weblog kann entweder von einem einzelnen Benutzer oder von einer Benutzergruppe geführt werden. Es wird dabei immer unter dem Kurznamen des jeweiligen Benutzer- oder Gruppen-Accounts verwaltet. Wer auf ein Weblog zugreifen, d.h. die Einträge lesen darf, wird durch den Autor des jeweiligen Weblogs bestimmt. In der Standardeinstellung darf jeder, der Zugriff auf den Webserver hat, also auch Fremde, die keine Weblog-Teilnehmer sind, die Blogs abrufen.

Mac OS X Server
Created with Mac OS X Server
Hans Schmitz's Weblog
Created with Mac OS X Server
Maria Schmitz's Weblog
Created with Mac OS X Server
Geben Sie Ihren Kurznamen ein und drücken Sie die Zeilenschaltung, um Ihr eigenes Weblog zu erstellen.
Geben Sie den Kurznamen der Gruppe ein und drücken Sie die Zeilenschaltung, um ein Weblog für diese Gruppe zu erstellen.

Abbildung 12.5: Auf der Startseite des Weblog-Dienstes werden die bereits vorhandenen Blogs aufgelistet. Sie können die Erstellung eines neuen Blogs vorbereiten, indem Sie in das Eingabefeld den Kurznamen eines Benutzers oder einer Benutzergruppe eintragen.

Die auf dem Webserver vorhandenen Blogs werden auf der Startseite des Weblog-Dienstes angezeigt. Um die Erstellung eines neuen Weblogs vorzubereiten, geben Sie Ihren Kurznamen oder den Namen einer Benutzergruppe in das Feld rechts unten ein (Abbildung 12.5). Beachten Sie, dass hierbei noch kein neues Blog angelegt wird. Das System prüft nur, ob ein Blog unter diesem Namen registriert ist und bereitet die mögliche Erstellung vor, falls kein Eintrag gefunden wird.

Um tatsächlich ein neues Blog zu erstellen, müssen Sie sich mit Namen und Kennwort am Weblog-Dienst anmelden. Es sei noch einmal darauf hingewiesen, dass das Kennwort nur dann sicher und verschlüsselt übertragen wird, wenn Sie https-Adressen statt http-Adressen verwenden. Es erscheint ein Anmeldedialog wie in Abbildung 12.6.

Nach der Anmeldung können Sie nun ein von Ihnen verfasstes Stück Text im Weblog veröffentlichen. Jede Textveröffentlichung wird *Eintrag* genannt. Falls Sie zu verschiedenen Themen Texte veröffentlichen möchten, können Sie Ihre Einträge auch unter selbst gewählten Oberbegriffen gruppieren. Ein solche Gruppierung wird *Kategorie* genannt. Sie können sich eine Kategorie als Ordner vorstellen, in dem Ihre Einträge liegen, und technisch ist er auch genau so realisiert. Wenn Sie einen Eintrag ohne Kategorisierung veröffentlichen, landet er im Stammordner Ihres Blogs. Wenn Sie eine Kategorie anlegen, wird intern ein Unterordner erzeugt, in den dann die Texte eingestellt werden.

Kategorien werden automatisch in der Leiste rechts aufgelistet falls vorhanden, und durch Anklicken können Sie in diese Kategorie navigieren. In jedem Fall ist der Link ALLE EINTRÄGE vorhanden, der zur Auflistung sämtlicher Einträge unabhängig von deren Kategorie führt. Wie erwähnt werden Blogs in Form eines Tagebuchs organisiert, deshalb ist als eigentliches Hauptsortierungskriterium der Einträge die Datums- und Uhrzeitangabe der Veröffentlichung anzusehen. In der Liste befindet sich deshalb ein Kalender, in dem Sie navigieren können, wodurch die entsprechenden Einträge herausgesucht werden. Auch ein Suchfeld zur Freitexteingabe ist

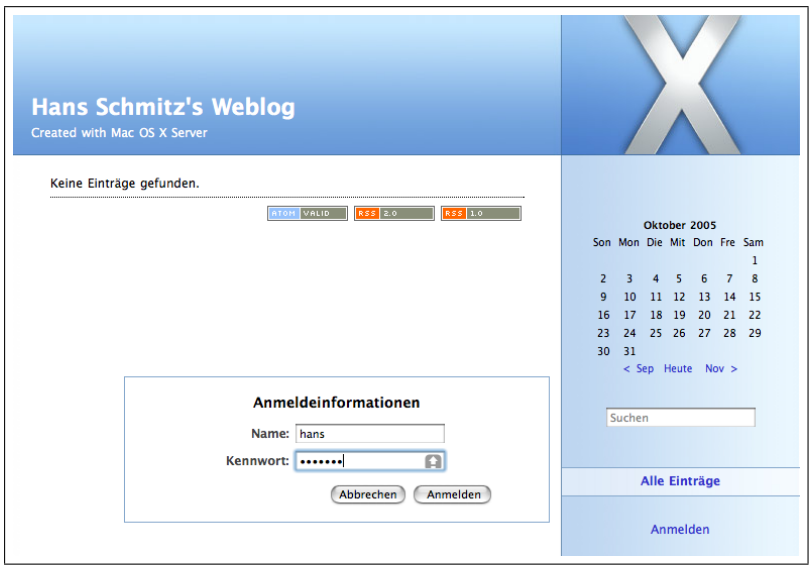

Abbildung 12.6: Um ein neues Weblog oder neue Einträge zu erstellen, müssen Sie sich anmelden.

vorhanden.

Sie können durch Anklicken der Punkte NEUE KATEGORIE und KATEGORIE LÖSCHEN neue Unterordner anlegen, bzw. sie wieder entfernen. Das Anklicken des Punktes NEUER EINTRAG führt schließlich zur wichtigsten Tätigkeit, nämlich dem Anlegen einer neuen Veröffentlichung. In einem Klappmenü werden Sie nochmals nach der Kategorie des neuen Eintrags gefragt und können sie falls nötig ändern. Ist der Eintrag unkategorisiert, wird dies durch den Stammordnerpfad / gekennzeichnet. Im Feld TITEL müssen Sie einen Titel für die Veröffentlichung eingeben. Die Angabe ist zwingend, da auf Basis des Titels die interne Ablage des Eintrags erfolgt. Im unbeschrifteten großen Kästchen können Sie schließlich den Text des Eintrags schreiben, der veröffentlicht werden soll.

Dies ist kein reiner Text, es stehen Ihnen zur Veröffentlichung viele Markierungselemente des HTML-Standards zur Verfügung. Sie dürfen folgende HTML-Tags verwenden: *a, b, blockquote, br, code, dd, dl, div, em, h1, h2, h3, h4, h5, h6, i, img, ol, lik, p, pre, span, strong, sub, sup, table, td, th, tr, u, ul*. Beachten Sie, dass das href-Tag zum Erstellen von Hyperlinks nicht in der Liste enthalten ist. Das System versucht stattdessen Hyperlinks, die Sie in den Text eingeben, automatisch zu erkennen, und erstellt daraus einen korrekten Link.

Sie können selbstverständlich auch Links verwenden, die auf andere Weblog-Einträge von Ihnen oder von anderen Autoren verweisen. Darüber hinaus gibt es in Weblogs aber noch eine zweite Art von Link, die verwendet werden kann: Eine sogenannte *Rückverbindung* oder *Trackback* ist ein Link, der in einem *fremden* Weblog-Eintrag an einer besonderen Stelle erscheint und dann auf *Ihren jetzigen*

Hans Schmitz's Weblog
Created with Mac OS X Server
Heh schaut mal!
Kategorie: Test-Weblog
Die Maria macht mir alles nach... :-(
Hans
Eintrag von: Hans Schmitz
@ 12. Oktober 2005 21:36:20 CEST (0 Kommentare | 0 Rückverbindungen (trackbacks))
# Bloggen ist cool!
Kategorie: Test-Weblog
Hallo Leute,
dies ist mein neuer Weblog!
Eintrag von: Hans Schmitz
@ 12. Oktober 2005 21:29:09 CEST (2 Kommentare | 0 Rückverbindungen (trackbacks))
Oktober 2005
Son Mon Die Mit Don Fre Sam
1
2 3 4 5 6 7 8
9 10 11 12 13 14 15
16 17 18 19 20 21 22
23 24 25 26 27 28 29
30 31
< Sep Heute Nov >
Suchen
Alle Einträge
Test-Weblog
Anmelden

Abbildung 12.7: Weblogs werden in einer schicken Oberfläche präsentiert. Die Einträge werden automatisch nach Datum und Uhrzeit sowie nach frei wählbaren Kategorien abgelegt.

Eintrag zurückverweist.

An einem Beispiel wird deutlicher, was gemeint ist: Nehmen wir an, Hans hat einen Blog-Eintrag von Maria gelesen und will in seinem eigenen Blog darauf Bezug nehmen. Wenn Hans einen neuen Eintrag erzeugt, in dem er Marias Eintrag kommentiert, kann er auf ganz normale Weise einen Link in seinem Eintrag setzen, der auf Marias Blog verweist. Er ist aber zusätzlich dazu berechtigt, auch *die Leser von Marias Blog* darauf hinzuweisen, dass er auf einen Eintrag von Maria Bezug nimmt. Hierzu legt Hans in seinem neuen Eintrag zusätzlich noch ein Trackback für Marias Eintrag an. Bei Marias Eintrag wird hierdurch eine abrufbare Markierung erscheinen, die wiederum auf den neuen Eintrag von Hans verweist. Dies kann sich in Diskussionen als nützliches Hilfsmittel erweisen, damit ein zweiseitiger Bezug – nicht nur eine einzige Verweisrichtung wie sonst üblicherweise im Web – entsteht.

Um ein Trackback zu erstellen müssen Sie folgende Schritte durchführen:

1. Rufen Sie den fremden Weblog-Eintrag auf, auf den Sie sich beziehen wollen.
2. Klicken Sie rechts unter dem Eintrag auf den Punkt RÜCKVERBINDUNG (TRACKBACK).
3. Verwenden Sie die Funktion BEARBEITEN | KOPIEREN in Ihrem Web-Browser, um die Internetadresse, die unter RÜCKVERBINDUNGS-URL FÜR DIESEN EINTRAG notiert ist, in die Zwischenablage zu kopieren (Abbildung 12.8).
4. Legen Sie einen neuen Eintrag in Ihrem eigenen Weblog an.

Maria Schmitz's Weblog
Created with Mac OS X Server
Titel: Na das kann ich auch.
Eintrag von: Maria Schmitz
Was der Hans kann, kann ich schon lange.
Grüße
Maria
Rückverbindungs-URL für diesen Eintrag:
http://www.example.private:16080/weblog/maria/?permalink=Nadaskannichauch.html&tb=y
@ 12. Oktober 2005 21:32:52 CEST (0 Kommentare | 0 Rückverbindungen (trackbacks))
ATOM VALID
RSS 2.0
RSS 1.0

Abbildung 12.8: Um die Adresse für einen Trackback zu ermitteln, müssen Sie den fremden Eintrag aufrufen und die URL als Rückverbindungs-URL in Ihren eigenen Eintrag kopieren.

5. Kopieren Sie den Inhalt der Zwischenablage in das Eingabefeld RÜCKVERBINDUNGS-URL.

6. Füllen Sie die restlichen Felder aus und speichern Sie Ihren neuen Eintrag ab.

Wenn Sie nun in den fremden Weblog-Eintrag zurückgehen, hat das Weblog-System automatisch unter RÜCKVERBINDUNG (TRACKBACK) einen neuen Verweis aufgezeichnet. Klicken Sie den Punkt nochmals an, so werden die Inhalte der Blogs, die auf diesen Eintrag verweisen, aufgelistet.

Blog-Einträge können auch kommentiert werden, wozu sich ein zweiter Link unter jedem Eintrag befindet. Die Kommentarmöglichkeit steht dabei allen Lesern eines Blogs offen. Das heißt, dass nicht nur die Blog-Teilnehmer, sondern auch Außenstehende, die keine Benutzerberechtigung auf dem Server haben, an der Diskussion teilnehmen können. Die Festlegung, wer Leserecht (und damit auch Kommentarrecht) für ein Blog hat, legt der Blog-Autor selbst fest, indem er den Punkt EINSTELLUNGEN in der rechten Leiste anklickt. Es erscheint ein Dialogfenster wie in Abbildung 12.9. Neben Titel, Untertitel und Stil des Weblogs, sowie Name und Mail-Adresse des Eigentümers steht die Tabelle LESER zur Verfügung, mit der die Zugriffsberechtigung gesteuert wird. Normalerweise ist die Tabelle leer, was bewirkt, dass keinerlei Zugriffsbeschränkungen bestehen, sondern alle Personen, die auf den Webserver zugreifen, das Blog einsehen und kommentieren können. Durch Eintippen von Kurznamen von Benutzern oder Gruppen wird dagegen eine Zugriffsbeschränkung eingerichtet und nur noch die aufgeführten Teilnehmer

Abbildung 12.9: Die Einstellungen für jedes Weblog werden vom Autor selbst vorgenommen. Eine Zugriffsbeschränkung kann auf Wunsch durch Ausfüllen der Tabelle LESER eingerichtet werden.

können das jeweilige Weblog aufrufen.

Neben der Präsentation der Blog-Inhalte auf Webseiten beherrscht Blojsom auch das Erzeugen von RSS-Feeds. Mit einem passenden Aggregator, z.B. einem RSS-fähigen Browser wie Safari können Sie die Weblogs auch in Form einer Zusammenfassung abrufen (Abbildung 12.10).

12.4 Instant Messaging mit dem iChat-Server

12.4.1 Einführung

Ebenso wie das Bloggen gehört auch das *Chatten* (englisch: *plaudern, schwätzen*) zu den „neumodischen" Kulturtechniken beim Austausch digitaler Nachrichten. Bei diesem auch als *Instant Messaging (IM)* bezeichneten Verfahren kommunizieren zwei oder mehr Partner über ein Netzwerk, indem sie live Textnachrichten austauschen, die im Moment des Tippens oder zeilenweise bei allen Kommunikationspartnern sichtbar werden. Auch das Austauschen von Internet-Adressen oder Dateien ist möglich. Diese Grundfunktionalität kann durch Einbeziehung von Audio-, beziehungsweise Audio- und Videosignalen ergänzt werden, falls die Kommunikationspartner hierzu technisch in der Lage sind. In Mac OS X liefert Apple das Programm *iChat* mit, das sämtliche üblichen Chat-Techniken beherrscht.

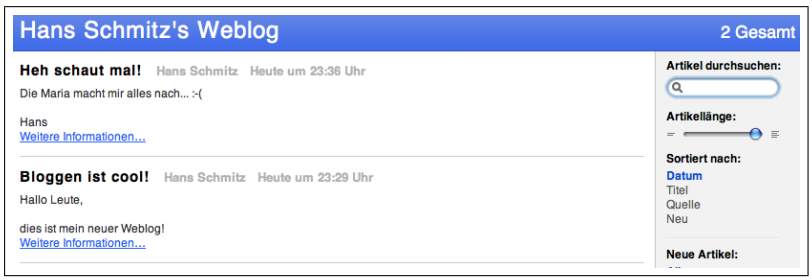

Abbildung 12.10: Blojsom kann Weblogs auch in Form von RSS-Feeds anbieten.

Der Aufbau einer Chat-Verbindung gleicht einem Telefonanruf, bzw. dem Aufbau einer Konferenzschaltung. Es muss daher eine Art Vermittlungsstelle geben, über den die Kommunikationspartner ihren Anrufwunsch äußern können, damit die entsprechenden Datenpakete an die richtige Stelle gesandt werden. Der Datenaustausch selbst wird zwar von den einzelnen Chat-Programmen übernommen, aber zum Zeitpunkt des Verbindungsaufbaus ist noch nicht bekannt, wo sich das jeweils „andere Ende" der Verbindung befindet. Zwar wäre es theoretisch denkbar, dass der Verbindungsaufbau durch Nennung des DNS-Namens oder der IP-Adresse des entfernt stehenden Rechners erfolgt, aber diese Daten können sich durch die Verwendung dynamischer IP-Adressen oder durch roamende Benutzer jederzeit ändern. Es wäre also nötig, vor dem Aufbau der Verbindung sich auf einem *anderen* Kommunikationskanal (Telefon, Fax, E-Mail...) erst über die technischen Details der Verbindungsaufnahme zu einigen, ein sehr unpraktisches Verfahren.

Aus diesem Grund wird beim Instant Messaging in der Regel ein spezieller Verzeichnisdienst verwendet, in dem alle potenziellen Teilnehmer registriert sind. Dies gleicht einem Telefonverzeichnis. Statt einer sich möglicherweise ständig ändernden IP-Adresse reicht es damit zur Kontaktaufnahme, einen *Chat-Namen* des gewünschten Kommunikationspartners anzugeben. Der Verzeichnisdienst ermittelt die technischen Details, wie der Partner momentan zu erreichen ist, und koordiniert als *Chat-Server* den Verbindungsaufbau. Apple stellt in Mac OS X Tiger Server einen solchen Dienst unter dem Namen *iChat-Server* bereit. Er wird in Wirklichkeit durch das quelloffene Programm *Jabber* (englisch: plappern) realisiert.

Wenn Sie iChat verwenden, um eine IM-Sitzung über das Internet aufzubauen, bietet Ihnen Apple normalerweise an, entweder ein Benutzerkonto in Apples *.Mac*-Dienst oder ein *AIM*-Benutzerkonto *(America Online Instant Messenger)* als Basis für die Vermittlung einzusetzen. Mit einem eigenen iChat-Server in Ihrem Hausnetz ist dies nicht mehr nötig, zumindest wenn Sie sich auf Kommunikationspartner im eigenen Netz beschränken. Gegenüber einem „großen" Chat-Verzeichnisdienst bietet ein privater iChat-Server die folgenden Vorteile:

- Die Nutzung ist kostenlos und nicht an fremde Nutzungsverträge gebunden.
- Die Chat-Teilnehmer werden durch Open Directory identifiziert, indem sie Name und Kennwort eingeben. Sie können daher in der Regel sicher sein, dass

Ihre Kommunikationspartner auch die sind, für die sie sich ausgeben.

- Wenn Sie auf dem Server ein SSL-Zertifikat hinterlegt haben, wird die Kommunikation verschlüsselt durchgeführt. Sie können daher auch vertrauliche Firmendaten im Chat diskutieren.

Der iChat-Server ist nicht auf Kommunikationspartner, die iChat nutzen, beschränkt. Auch mit fremden Chat-Programmen und anderen Betriebssystemen wie Linux und Windows können Chats über den iChat-Server vermittelt werden, solange sie das Kommunikationsprotokoll *Jabber* / *XMMP* unterstützen. Auch einige PDA-Computer beherrschen diese Technik. XMMP bedeutet *Extensible Messaging and Presence Protocol* und ist ein Internet-Standard für Chat-Dienste, der aus dem Jabber-Projekt heraus entstanden ist. XMMP basiert auf XML-Technologien und ist in den Internetstandards RFC 3920 und RFC 3921 definiert.

Der Server-Dienst wird durch das Programm *jabberd (Jabber Daemon)* realisiert, der sich an der Stelle

```
/usr/sbin/jabberd
```

befindet. Die Konfiguration des Servers wird durch eine XML-Datei an der Position

```
/etc/jabber/jabber.xml
```

gespeichert. Im Normalfall reicht es aber aus, das Programm Server Admin zur Einrichtung des IM-Dienstes zu verwenden. Falls Sie detaillierte Informationen zum Jabber-Projekt oder zum Programm jabberd benötigen, können Sie die offiziellen Webseiten

```
http://www.jabber.org/
http://jabberd.jabberstudio.org/
```

besuchen.

12.4.2 Einrichten des Chat-Servers

Ähnlich wie bei Blojsom ist die Einrichtung von Jabber aus Sicht des Administrators auf wenige Schritte beschränkt und denkbar einfach:

1. Starten Sie Server Admin und verbinden Sie sich mit dem Server, auf dem die IM-Dienste laufen sollen.
2. Wählen Sie in der Tabelle COMPUTER & DIENSTE den Punkt ICHAT aus.
3. Gehen Sie im rechten Teil des Fensters zum Punkt EINSTELLUNGEN.

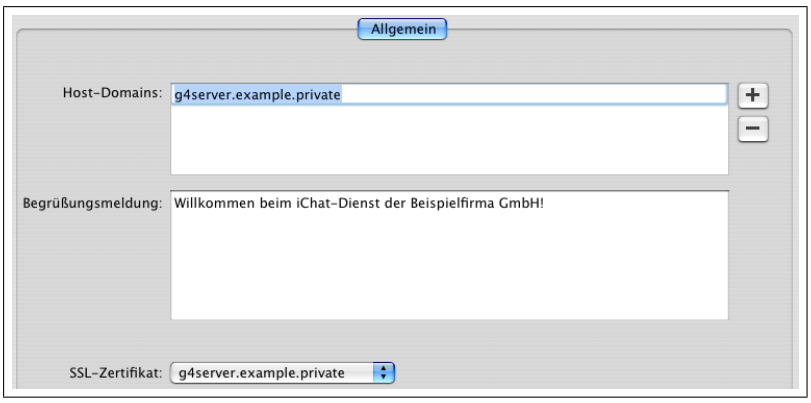

Abbildung 12.11: Die Einrichtung des iChat-Servers ist sehr übersichtlich: Es reicht aus, den Domain-Namen, eine Begrüßungsmeldung und eventuell ein SSL-Zertifikat anzugeben.

Es erscheint die Anzeige aus Abbildung 12.11. Geben Sie im oberen Feld HOST-DOMAINS mindestens einen Domänennamen an, unter dem Jabber die einzelnen Benutzerkonten führen soll. Auf Chat-Benutzer wird durch Adressen der Form

```
benutzer@domänenname
```

Bezug genommen. Diese Adressen sehen wie E-Mail-Adressen aus, müssen aber nicht mit ihnen identisch sein. Sie dienen als *Pseudonym (Nickname)* der Chat-Benutzer, wobei allerdings schon festgelegt ist, dass es sich beim Benutzernamen um den Kurznamen des Accounts um beim Domänennamen um eine gültige DNS-Namen des Servers handeln muss. Befindet sich der Server in mehreren DNS-Domänen oder weist er Aliasnamen auf, können weitere Einträge über die Plus-Taste in die Tabelle eingefügt werden.

Im Feld BEGRÜSSUNGSMELDUNG können Sie eine mehrzeilige Meldung definieren, die den Chat-Partnern nach erfolgreichem Aufbau der Verbindung angezeigt wird. Im Feld SSL-ZERTIFIKAT wählen Sie ein Zertifikat aus, das für die SSL-Verschlüsselung verwendet werden soll. Das Klappmenü bietet Ihnen automatisch die Zertifikate an, die Sie – wie in Abschnitt 9.3 beschrieben – in Server Admin eingerichtet haben. Über den Knopf in der Symbolleiste können Sie den Chat-Server starten oder stoppen. Berichte über den Betrieb des Jabber-Dienstes können Sie bekommen, indem Sie den Punkt PROTKOLL am unteren Fensterrand aufrufen.

12.4.3 Verwendung von iChat

Haben Sie einen privaten iChat-Server erfolgreich eingerichtet, können Ihre Benutzer an hausinternen Chats mit iChat oder anderen XMMP-Programmen teilnehmen. Der typische Aufbau einer iChat-Sitzung läuft folgendermaßen ab:

1. Starten Sie das Programm *iChat*. Es befindet sich im Programme-Ordner.

2. Falls Sie das Programm in diesem Benutzer-Account zum ersten Mal verwenden, erscheint ein Begrüßungsfenster. Betätigen Sie die Schaltfläche FORTFAHREN.

3. Es erscheint das Fenster ICHAT INSTANT MESSAGING KONFIGURIEREN. Sie sollten an dieser Stelle Ihren Namen und Vornamen in die entsprechenden Felder eintragen. Das Ausfüllen der anderen Felder ist für hausinternes Messaging über den iChat-Server unnötig. Betätigen Sie die Taste FORTFAHREN.

4. Es erscheint das Fenster JABBER INSTANT MESSAGING KONFIGURIEREN (Abbildung 12.12). Kreuzen Sie bitte den Punkt JABBER INSTANT MESSAGING VERWENDEN an und geben Ihren Benutzernamen und Kennwort ein. Das Kennwort ist Ihr normales Open Directory-Kennwort, der Benutzername ist jedoch Ihr Chat-Pseudonym. Wie oben beschrieben muss er nach dem Prinzip *kurzname@server* aufgebaut sein, z.B. *hans@g4server.example.private*.

5. Falls Sie zum Aufbau der Vermittlung wahlweise auch Bonjour nutzen möchten, können Sie dies im nächsten Bild aktivieren.

6. Im nächsten Bild können Sie (falls vorhanden und falls gewünscht) eine Kamera für den Aufbau einer Videokonferenz konfigurieren. Ebenso wird durch einen horizontalen Balken die Stärke des vorhandenen Audiosignals symbolisiert, falls Ihr Computer mit einem Mikrofon ausgestattet ist. Die Konfiguration von Bild und Ton muss über andere Programme, z.B. die iSight-Software und Systemeinstellungen erfolgen. Drücken Sie nach Abschluss der Konfiguration von Audio und Video auf FORTFAHREN.

7. Bestätigen Sie das letzte Bild mit FERTIG.

Wenn mindestens zwei Benutzer diese Konfigurationsschritte ausgeführt haben, kann eine Chat-Sitzung eröffnet werden.

1. Betätigen Sie im Fenster JABBER LISTE von iChat den Knopf mit dem Pluszeichen links unten.

2. Drücken Sie im erscheinenden Dialogfenster den Knopf NEUE PERSON.

3. Geben Sie das iChat-Pseudonym des Benutzers ein, den Sie kontaktieren möchten. Sie können auf Wunsch auch ein Symbol, Vorname, Nachname und E-Mail-Adresse dieses Benutzers eingeben, um den Kontakt netter zu gestalten.

4. Die Person wird in die Tabelle aufgenommen. Durch Auswählen des Eintrags und Druck auf die Taste mit dem Symbol A unterhalb der Tabelle können Sie einen Chat-Sitzung im Textmodus zum angegebenen Partner aufbauen. Durch Druck auf die anderen Symbole können entsprechend Audio und Video dem Chat hinzugefügt werden, falls die technischen Voraussetzungen gegeben sind.

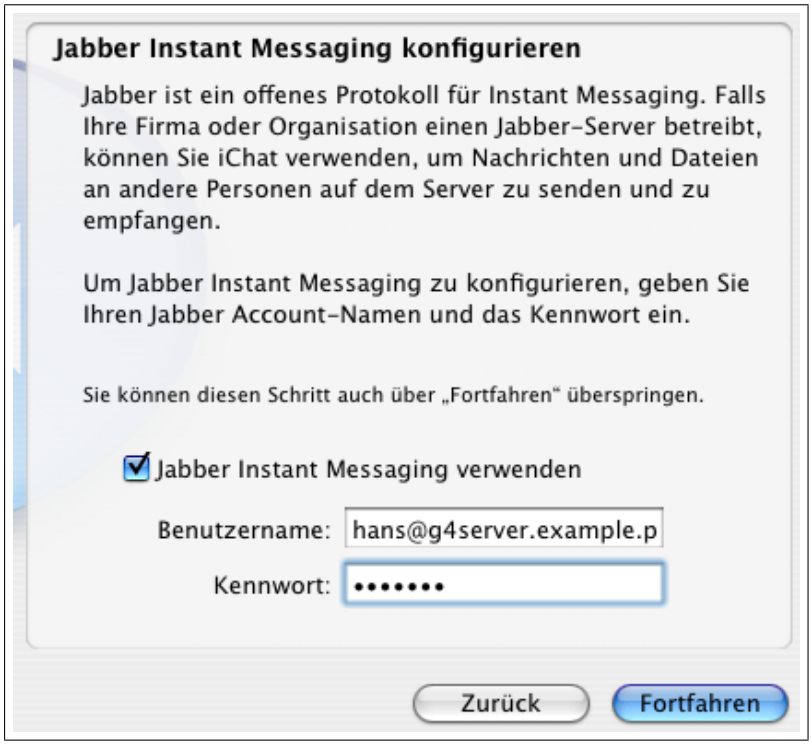
Jabber Instant Messaging konfigurieren
Jabber ist ein offenes Protokoll für Instant Messaging. Falls Ihre Firma oder Organisation einen Jabber-Server betreibt, können Sie iChat verwenden, um Nachrichten und Dateien an andere Personen auf dem Server zu senden und zu empfangen.
Um Jabber Instant Messaging zu konfigurieren, geben Sie Ihren Jabber Account-Namen und das Kennwort ein.
Sie können diesen Schritt auch über „Fortfahren" überspringen.
Jabber Instant Messaging verwenden
Benutzername: hans@g4server.example.p
Kennwort: •••••••
Zurück
Fortfahren

Abbildung 12.12: Die Daten für die Verbindungsaufnahme über den Jabber-Server werden in iChat eingegeben.

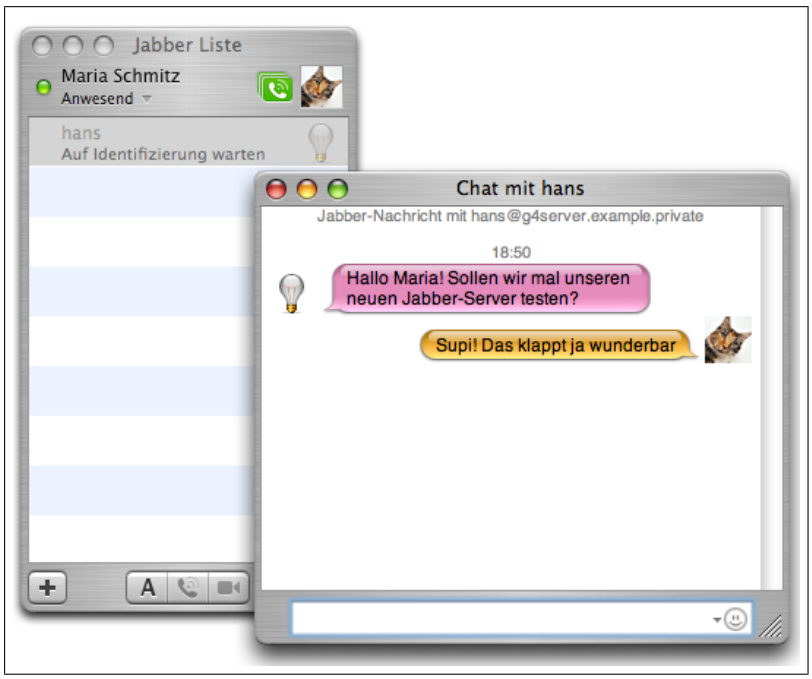

Abbildung 12.13: Der erfolgreiche Aufbau einer iChat-Sitzung über Jabber.

5. Auf dem Bildschirm des anderen Benutzers erscheint ein Fenster JABBER-IDENTIFIZIERUNG nachdem er auch iChat gestartet hat. Wird die Anfrage durch Druck auf die Taste AKZEPTIEREN in diesem Fenster bejaht, wird auch in umgekehrter Richtung ein Kontakteintrag, diesmal für den anderen Benutzer, erstellt.

6. Führt einer der beiden Benutzer einen Doppelklick auf den Personeneintrag des Anderen in der Jabber-Liste aus, so erscheint ein Chat-Fenster und die Verbindung wird aufgebaut.

Selbstverständlich können wir an dieser Stelle kein vollständiges Benutzerhandbuch für iChat liefern, aber der Verbindungsaufbau über Jabber sollte damit verständlich geworden sein.

12.5 QuickTime Streaming Server

12.5.1 Neuerungen

Apple hat das QuickTime Streaming-System in Tiger von QuickTime 6 auf den Stand von QuickTime 7 aktualisiert. Das heißt, dass einige neue Codecs und Datenformate für die Videodatenströme zur Verfügung stehen:

- Es wird das Streaming von Daten im *3GPP*-Format *(3rd Generation Partnership Project)* unterstützt. Die entsprechenden 3gp-Dateien sind zum Industriestandard für das Streamen von Videodaten auf Mobiltelefonen geworden.
- QTSS ist in der Lage, die *HD*-Filmformate *(High Definition)* zu unterstützen, die sich in der Zukunft als Standard für Film und Fernsehen durchsetzen werden.
- Die neue Norm *ITU-T H.264* zur Komprimierung von hochauflösenden Videodaten, auch bekannt als *MPEG-4 Teil 10* oder *ISO 14496-10* wird unterstützt.

Das zu Tiger gehörige QTSS trägt nun die Versionsnummer 5.5. Bezüglich des quelloffenen Kerns von QTSS, dem *Darwin Streaming Server* hat Apple inzwischen die Unterstützung der Plattformen Microsoft Windows NT und SUN Solaris aufgegeben. Es werden damit neben Mac OS X (ab 10.3.9) noch Linux (in der Distribution Red Hat Version 9), Microsoft Windows 2000 Server und Microsoft Windows Server 2003 unterstützt.

Neben diesen technologischen Verbesserungen liefert Apple eine komplett neue Version des *QTSS Publisher* mit Tiger Server zusammen aus. Besitzer der Standardversion von Mac OS X können das Programm unter der im Hauptbuch genannten Adresse im Internet herunterladen. Statt *1.0 (v33)* trägt die neue Version des Programms nun die Nummer *10.4 (66)*. Wir werden im Folgenden die im Hauptbuch genannten Beispiele zur Einarbeitung in die QTSS-Technik noch einmal anhand der neuen Programmversion durchspielen.

An der Steuerung des QuickTime Streaming Servers in Server Admin hat sich kaum etwas geändert. Genannt werden sollte eine wichtige Neuerung des QTSS, nämlich dass Benutzer nun selbständig in ihrem eigenen Privatordner Streaming-Medien veröffentlichen dürfen. Hierzu sind folgende Schritte durchzuführen:

1. Starten Sie Server Admin und verbinden Sie sich mit dem Server, auf dem QTSS läuft.
2. Wählen Sie in der Tabelle COMPUTER & DIENSTE den Punkt QUICKTIME STREAMING aus.
3. Gehen Sie im rechten Teil des Fensters zum Punkt EINSTELLUNGEN und dort zu ZUGRIFF.
4. Kreuzen Sie den Punkt STREAMING VON „PRIVAT"-ORDNERN ERLAUBEN an.
5. Betätigen Sie die Schaltfläche SICHERN.

Wenn ein Benutzer nun einen Unterordner

```
Sites/Streaming
```

in seinem privaten Ordner anlegt (und die Privatordner der Nutzer zentral auf dem Server abgelegt sind), so kann er dort streaming-fähige Mediendateien ablegen, die von QTSS automatisch im Netz angeboten werden. Zum Abruf der Medien sind Adressen nach dem Prinzip

```
rtsp://server/~benutzerkurzname/mediendatei.mov
```

zu verwenden. Der Ablageort für Medien im Web-Datenbereich des Servers wird innerhalb von QTSS *Systembibliothek*, die Ablage im Privatordner BENUTZERBIBLIOTHEK genannt.

12.5.2 Fallbeispiele: Streaming und Erzeugung von Webseiten

Um den Umgang mit dem neuen QTSS Publisher noch einmal an den im Buch genannten Fallbeispielen zu verdeutlichen, wiederholen wir die Schritte mit der aktuellen Version 10.4. Wir gehen davon aus, dass die QuickTime-Dateien bereits als *Stream mit Steuerspur* transkodiert wurden.

Live-Übertragung einrichten

Starten Sie den QTSS Publisher und melden Sie sich über das Programm an einem Server an, auf dem der QTSS aktiviert ist.

Ziehen Sie dann Ihre beiden streaming-fähigen Filmdateien über das Symbol BIBLIOTHEK in der linken Tabelle QUELLE des Fensters. Hierdurch werden die Filme vom Publisher überprüft und über das Netzwerk auf den QTSS-Computer übertragen. Während der Übertragung, die einige Zeit in Anspruch nehmen kann, erscheinen kleine blaue Synchronisationssymbole neben den betreffenden Einträgen (Abbildung 12.14). Der Vorgang ist erfolgreich abgeschlossen, wenn die blauen Symbole verschwinden und in der Spalte DATENRATE ein Wert angezeigt wird. Wird kein Wert angezeigt, ist die Datei nicht akzeptiert worden, z.B. wenn die Datenrate viel zu hoch ist oder ein ungültiger Codec eingesetzt wurde.

Wir möchten mit den beiden Dateien Folgendes machen: Zum einen wollen wir eine Web-Seite einrichten, auf denen die beiden Dateien immer wieder hintereinander als Live-Sendung abgespielt werden. Zum anderen wollen wir zwei weitere Web-Seiten erstellen, auf denen jede Datei *on demand* gestreamt wird, d.h. der Benutzer kann den Film anklicken, worauf er von Anfang bis Ende abgespielt wird.

Damit wir aus den beiden Filmen ein Live-Programm machen können, das endlos abgespielt wird, müssen wir eine Wiedergabeliste erstellen: Drücken Sie in der Symbolleiste die Schaltfläche NEUE MEDIEN-WIEDERGABELISTE. Geben Sie im erscheinenden Dialogfenster NAME und URL-NAME ein. Der Name ist ein beliebiger Titel, der für die Wiedergabeliste vergeben wird, der URL-Name wird später verwendet, um Dateinamen für verschiedene Web-Dokumente zu erzeugen, deshalb darf er keine Leer- oder Sonderzeichen enthalten. Betätigen Sie dann die Schaltfläche ERSTELLEN.

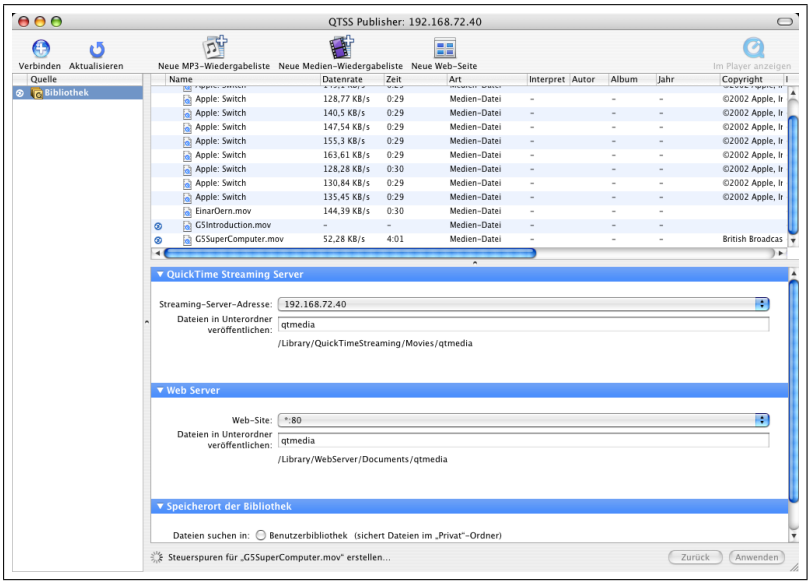

Abbildung 12.14: Die beiden Testfilme werden in die Medien-Bibliothek einsortiert und auf den QTSS übertragen.

Markieren Sie nun die beiden Filme in der rechten Tabelle und ziehen Sie diese mit der Maus nach links über das neu eingefügte Symbol der Wiedergabeliste. Es trägt den Namen, den Sie gerade eingegeben haben. Wählen Sie danach das Symbol der Wiedergabeliste aus. Die rechte Hälfte des Fensters verändert sich und zeigt nun die Einstellungen für die Wiedergabeliste an. Stellen Sie bitte unter EINSTELLUNGEN DER WIEDERGABELISTE bei WIEDERGABEMODUS den Wert ENDLOS SEQUENZIELL ein und betätigen Sie die Taste ANWENDEN rechts unten. Um die Wiedergabe einzuleiten, drücken Sie den Knopf START unter dem Punkt BROADCAST-STATUS.

Falls Sie eine Meldung erhalten, dass „der Server einen Fehler zurückmeldet", sollten Sie noch einmal kontrollieren, ob es sich bei den Videodateien tatsächlich um Streams mit Steuerspur handelt, nicht um „normale" Videodateien. Leider sind die vom QTSS Publisher zurückgelieferten Fehlermeldungen wenig hilfreich. Genauere Meldungen finden Sie eventuell, wenn Sie auf dem Server selbst in den Dateien

```
/Library/Application Support/Apple/QTSS Publisher/Playlists/<playlist>/<playlist>.err
/Library/Application Support/Apple/QTSS Publisher/Playlists/<playlist>/<playlist>.log
```

nach Einträgen suchen. Aber auch hier sind Meldungen oft rätselhaft und bestehen z.B. nur aus dem Hinweis *error 15* oder ähnlichem.

Um die Live-Sendung zu sehen, können Sie den QuickTime-Player auf einem Rechner im Netz starten. Wählen Sie ABLAGE | URL ÖFFNEN... aus und geben Sie die Adresse ein, die Sie im QTSS Publisher unter STREAMING-LINK: URL angezeigt bekommen. Es handelt sich um URLs nach dem Muster

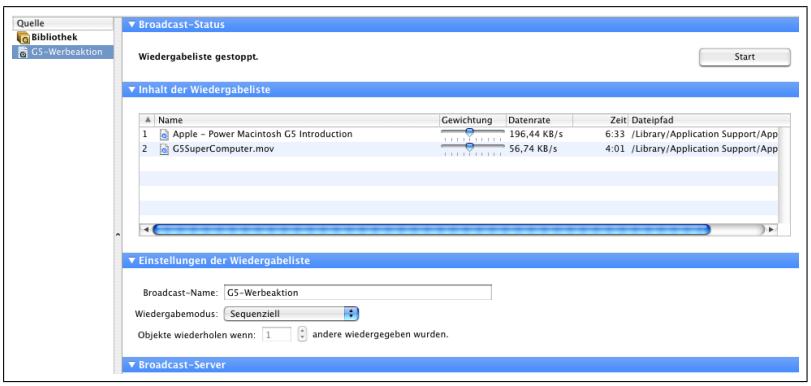

Abbildung 12.15: Das Live-Programm wird zusammengestellt. Die Bedienungsschritte sind ähnlich einfach wie bei iTunes.

```
rtsp://server/wiedergabeliste.sdp
```

Hierbei ist *server* durch den DNS-Namen des QTSS und *wiedergabeliste* durch den URL-Namen zu ersetzen, den Sie festgelegt hatten. Sie können ausprobieren, den Stream von mehreren Client-Computern in Ihrem Netz abzurufen. Die Player müssten alle ungefähr die gleiche Stelle des Films wiedergeben, woraus Sie sehen können, dass es sich um eine echte Direktübertragung handelt.

Wir gehen nun noch einen Schritt weiter und sorgen dafür, dass der Live-Stream auch innerhalb einer Webseite abrufbar wird. Rollen Sie in der rechten Hälfte des Publisher-Fensters noch einmal hinunter zum Punkt STREAMING-LINK und schalten Sie das Klappmenü AKTION AUF WEB-SEITE auf IN DIE WEB-SEITE EINBETTEN. Geben Sie bei ÜBERSCHRIFT AUF WEB-SEITE einen kurzen Text ein, der als Überschrift dienen soll und betätigen Sie die Schaltfläche ANWENDEN.

Auch für ein Miniaturbild, das als statische Vorschau auf dieser Webseite erscheint, solange das Video noch nicht läuft, lässt sich sorgen. Sie können es im QTSS Publisher unter MINIATUR | WÄHLEN nach Ihren Wünschen angeben. Tun Sie dies nicht, generiert der Publisher automatisch für Sie eine PNG-Datei, indem das erste Bild des Videos verwendet wird.

Drücken Sie nun in der Symbolleiste die Schaltfläche NEUE WEB-SEITE. Geben Sie im erscheinenden Dialogfenster bei NAME eine Überschrift für die Seite ein. Unter URL-NAME ist der Dateiname für das zu erstellende HTML-Dokument anzugeben. Drücken Sie nun auf ERSTELLEN, erscheint in der linken Tabelle unter dem eingegebenen Namen ein neuer Punkt, markiert mit dem Mac OS X-Symbol für einen Weblink. Gleichzeitig wurde im Hintergrund bereits ein HTML-Dokument in den folgenden Ordner Ihres Web-Servers gelegt:

```
/Library/WebServer/Documents/qtmedia
```

Wählen Sie nun das neue Symbol in der Tabelle QUELLE an. Die Anzeige des Pub-

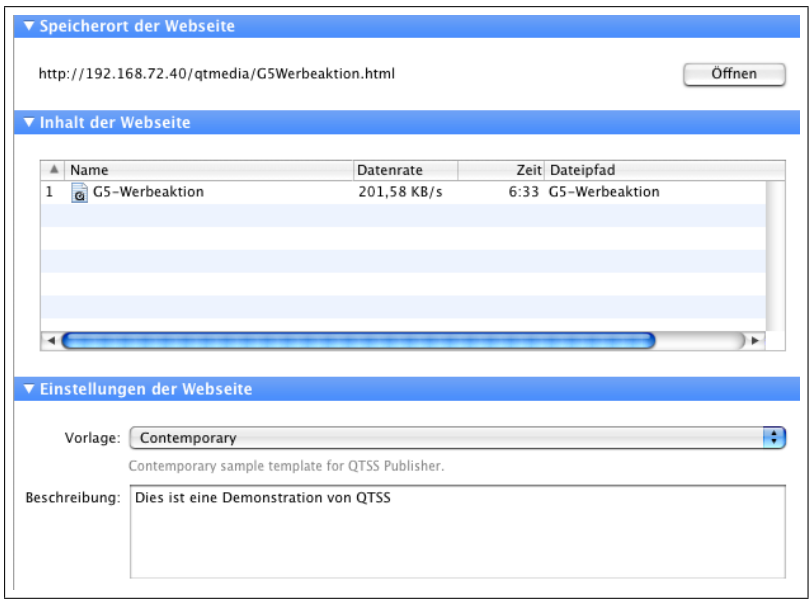

Abbildung 12.16: Die Daten für die zu erstellende Web-Seite werden eingegeben.

lishers verändert sich und erlaubt nun, Details für die neue Web-Seite einzugeben. Als erstes müssen wir noch einmal bestätigen, dass unsere Wiedergabeliste tatsächlich in die neue Web-Seite eingeblendet werden soll. Sie müssen hierzu sicher stellen, dass die Wiedergabeliste immer noch im Sendezustand ist (der Broadcast-Status lautet „wird gesendet“ und neben dem Listensymbol erscheint ein hellblaues Sendesymbol). Ziehen Sie in der Tabelle QUELLE das Symbol der Wiedergabeliste auf das Symbol der Web-Seite. Danach wird die Liste in der Tabelle INHALT DER WEBSEITE angezeigt (Abbildung 12.16). Beim Punkt BESCHREIBUNG können Sie einen Text eingeben, der auf der Seite unterhalb des Videos erscheinen soll. Betätigen Sie zum Schluss die Schaltfläche ANWENDEN rechts unten und drücken oben auf der Seite unter SPEICHERORT DER WEBSEITE auf ÖFFNEN.

Die Web-Seite wird generiert, auf den Server geschickt und Ihr Standard-Web-Browser geöffnet, der zugleich die neue Seite anzeigt. Abbildung 12.17 zeigt das Endergebnis in Safari. Wie bereits im Hauptbuch erwähnt, erzeugt der QTSS Publisher allerdings immer noch HTML-Code mit einigen Unstimmigkeiten, wie nicht zueinander passenden Bildgrößen von Miniatur, Filmgröße und Player. In Version 10.4 ist dies nicht besser geworden, hier werden auch teilweise die Überschriften falsch übernommen.

Beachten Sie, dass die Live-Übertragung, wenn auch nur geringfügig, Rechenzeit auf Ihrem Server beansprucht. Nach Abschluss des Tests sollten Sie über den STOPP-Knopf unter BROADCAST-STATUS der Wiedergabeliste die Übertragung beenden.

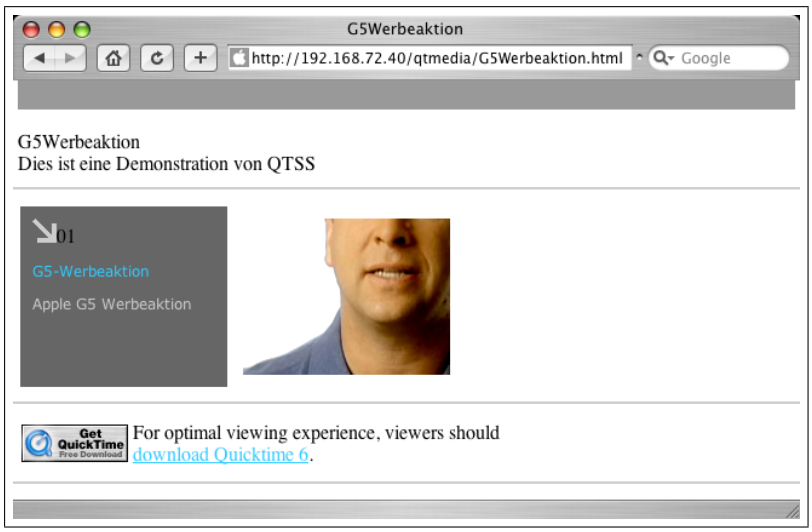

Abbildung 12.17: Der erste selbst definierte Live-Stream in Aktion. Die Qualität des HTML-Codes für die Web-Seite ist allerdings wenig überzeugend. So gut wie nichts funktioniert auf Anhieb.

Web-Seiten für Streaming erstellen

Um unsere zwei Web-Seiten für On-Demand-Streaming zu erstellen, müssen wir wieder in den QTSS Publisher zurückgehen. Wählen Sie in der Spalte QUELLE den Punkt BIBLIOTHEK und in der Übersichtstabelle eine der beiden Filmdateien aus.

1. Rollen Sie den unteren Bereich des Fensters nach unten, bis Sie den Punkt STREAMING-LINK sehen. Kreuzen Sie dort den Punkt MEDIENDATEI MIT QUICKTIME STREAMING SERVER VERÖFFENTLICHEN (SOFORTIGE WIEDERGABE) an.
2. Stellen Sie den Punkt AKTION AUF WEB-SEITE auf IN DIE WEB-SEITE EINBETTEN.
3. Geben Sie bei ÜBERSCHRIFT AUF WEB-SEITE einen Text für die Überschrift an.
4. Klicken Sie auf die Schaltfläche ANWENDEN rechts unten und warten Sie, bis ein Sendesymbol links neben dem Filmeintrag in der oberen Tabelle erscheint. Dies kann mehrere Minuten dauern.
5. Klicken Sie in der Symbolleiste auf NEUE WEB-SEITE.
6. Geben Sie wie schon bekannt NAME und URL-NAME für die neue Webseite ein. Sie dürfen keinen Namen einer bereits bestehenden Seite verwenden, da diese sonst ohne Warnung überschrieben wird.
7. Ziehen Sie das Symbol des Films aus der Tabelle über das Symbol der neuen Web-Seite in der Spalte QUELLE.

8. Klicken Sie das Symbol der neuen Web-Seite in der Spalte QUELLE an.
9. Geben Sie auf der rechten Seite einen Text in das Kästchen BESCHREIBUNG ein und stellen Sie den Punkt VORLAGE auf MODERN um.
10. Drücken Sie die Schaltfläche ANWENDEN rechts unten.
11. Klicken Sie auf den Knopf ÖFFNEN rechts oben.

Die Web-Seite wird generiert und in Ihrem Standardbrowser angezeigt. Sie können zur Übung den Vorgang mit der zweiten Datei wiederholen.

Kapitel 13

Fernstart – die NetBoot-Funktion

Am Grundprinzip des NetBoot-Verfahrens hat sich auch in Tiger nichts geändert. Sie sollten allerdings darauf achten, mindestens 10.4.2 Server, besser eine höhere Version, auf dem NetBoot-Server einzusetzen, da es in den ersten Fassungen größere Fehler bis hin zum Totalausfall von NetBoot gab.

13.1 Änderungen in Server Admin

Bezüglich der Verwaltung von NetBoot im Server Admin-Programm sind nur Kleinigkeiten zu vermelden. Eine nett gestaltete neues Anzeige unter NETBOOT | ÜBERSICHT zeigt nun tabellarisch an, welche Basisdienste für die einzelnen NetBoot-Funktionen notwendig sind, und ob diese momentan laufen (Abbildung 13.1).

Der neue Unterpunkt PROTOKOLLE erlaubt es, bei den EINSTELLUNGEN die gewünschte Ausführlichkeit des Verlaufsberichts der NetBoot-Tätigkeiten anzugeben. Ein neues Eingabefeld unter EINSTELLUNGEN | ALLGEMEIN erlaubt es schließlich, die Höchstzahl an AFP-Verbindungen festzulegen, die für das Booten von alten Mac OS-Klienten oder von plattenlosen Klienten auf dem jeweiligen Server beansprucht werden dürfen.

13.2 Das neue System-Image-Dienstprogramm

Das Programm zum Erstellen von NetBoot-Image-Dateien wurden dagegen in sehr vielen Punkten überarbeitet. Die erste Neuerung betrifft die Tatsache, dass das Programm statt *Netzwerk-Image-Dienstprogramm* jetzt *System-Image-Dienstprogramm* heißt.

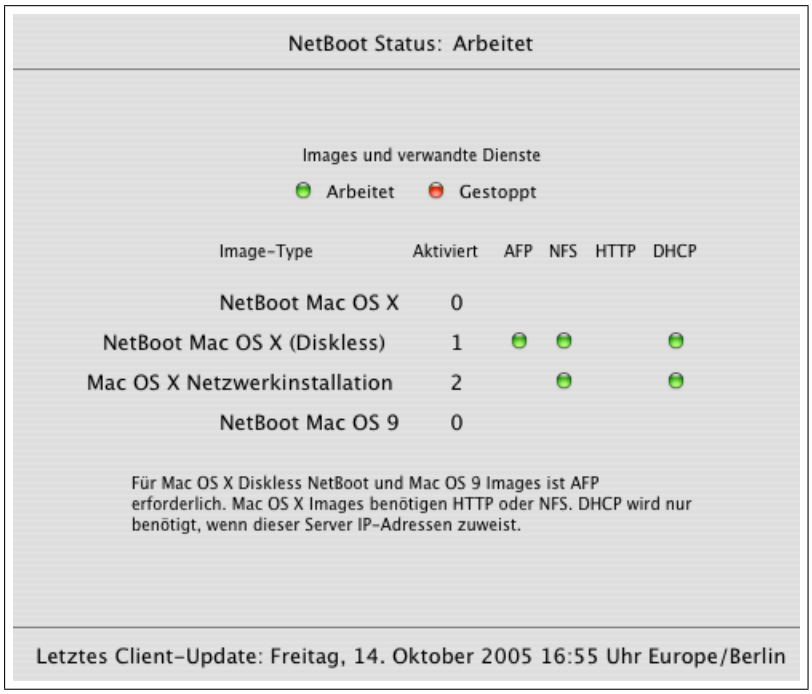
NetBoot Status: Arbeitet
Images und verwandte Dienste
Arbeitet
Gestoppt
Image-Type
Aktiviert
AFP
NFS
HTTP
DHCP
NetBoot Mac OS X 0
NetBoot Mac OS X (Diskless) 1
Mac OS X Netzwerkinstallation 2
NetBoot Mac OS 9 0
Für Mac OS X Diskless NetBoot und Mac OS 9 Images ist AFP erforderlich. Mac OS X Images benötigen HTTP oder NFS. DHCP wird nur benötigt, wenn dieser Server IP-Adressen zuweist.
Letztes Client-Update: Freitag, 14. Oktober 2005 16:55 Uhr Europe/Berlin

Abbildung 13.1: Die vielen Einzeldienste, die an der Realisation von NetBoot mitwirken, und deren Zustand werden jetzt in einer hübschen Tabelle dargestellt.

Ebenso wurde die Stabilität und Zuverlässigkeit des Programms stark verbessert. Es ist jetzt nicht mehr nötig, als root-Benutzer angemeldet zu sein, damit das Programm wie erwartet funktioniert. Neue Funktionen machen es außerdem möglich, vorzukonfigurieren, wie ein „ferngestarteter" Computer seinen eigenen Namen ermitteln soll und an welchen Verzeichnisdienst er sich zu binden hat. Ein Modellfilter erfüllt die Funktion, ein Netboot-Image so zu erstellen, dass es nur auf bestimmten Typen von Apple-Computern genutzt werden kann. Auf diese Weise können zum Beispiel Computer für den Start von Tiger ausgeschlossen werden, die mit Mac OS X 10.4 gar nicht kompatibel sind.

Eine weitere neue Funktion besteht darin, dass nun auch die grafische Oberfläche die Funktion beherrscht, ein Image so zu anzulegen, dass es nicht auf dem Server liegen muss, der als NetBoot-Server dient, sondern auf einem anderen NFS- oder HTTP-Fileserver platziert werden kann. Hierzu wird ein indirekter Mountverweis in den entsprechenden NetBoot-Image-Ordner eingefügt. Dies war früher nur über die Kommandozeile möglich.

Die in Kapitel 13.5 des Hauptbuchs zu findende Anleitung zur Erstellung von NetBoot-Image-Dateien ist in folgenden Punkten zu ergänzen:

- Da die Einstellung der Sprache zum Booten des Systems erst vorgenommen werden konnte, nachdem bereits die Quelle für das Image ausgewählt war, hat Apple konsequenterweise die Einstellung SPRACHE von der Karteikarte ALLGEMEIN auf die Karteikarte INHALT verschoben. Wenn man die Eingaben zur Erstellung des Images jetzt von oben nach unten und links nach rechts abarbeitet, steht der Punkt SPRACHE nun an der richtigen Stelle.

- Über die neuen Auswahlknöpfe PFAD ZUM IMAGE kann angegebenen werden, ob das Image später auf dem gleichen Server liegt, über den die NetBoot-Funktionen verwaltet werden. Bei der Einstellung LOKAL verhält sich das Programm wie früher. In diesem Fall muss der Server, der als NetBoot-Server arbeitet, auch als NFS- oder HTTP-Server arbeiten, von dem das letztendliche Boot-Image später geladen wird. Über die Einstellung ENTFERNT haben Sie die Möglichkeit, in den NetBoot-Image-Ordner einen Verweis auf einen *fremden* Fileserver einzufügen. Vorsicht: Apples Namensgebung bei dieser Funktion ist sehr verwirrend. Man könnte den Eindruck erhalten, der NetBoot-Image-Ordner würde direkt vom System-Image-Dienstprogramm aus auf einem entfernt stehenden Server abgelegt und Sie könnten sich den Vorgang des Hochladens des Images auf den Server sparen, falls das System-Image-Dienstprogramm nicht auf dem Computer läuft, der der NetBoot-Server ist. *Dies ist nicht der Fall!* Das System-Image-Dienstprogramm legt den erstellten NetBoot-Image-Ordner immer auf dem Rechner ab, auf dem es gerade läuft. Den Ordner an die richtige Stelle zu kopieren, liegt immer in Ihrer Verantwortung. Die Einstellung PFAD ZUM IMAGE legt fest, *ob während des späteren NetBoot-Vorgangs ein frei definierbarer Mountpfad zu einem fremden NFS- oder HTTP-Server* gewählt werden soll.

- Die Strategie, welche Installationspakete eines Betriebssystems ausgewählt werden, wenn Sie ein Installations-Image erstellen, hat sich geändert. Sie

hängt darüber hinaus von der Image-Quelle ab, die Sie angeben:

  - Wenn Sie ein Installations-Image zur Installation von Jaguar erstellen, enthält das Image grundsätzlich sämtliche Pakete der Jaguar-CDs. Da die Image-Datei hierbei sehr groß werden kann, empfiehlt Apple in diesem Fall den Punkt EINSTELLUNGEN | BEIM ERSTELLEN ODER BEARBEITEN KOMPRIMIEREN im System-Image-Dienstprogramm einzuschalten. Es sei noch einmal daran erinnert, dass bestimmte Firmware-Versionen und HTTP-Server damit Probleme haben, Image-Dateien zu verarbeiten, die größer als 2 GByte sind.
  - Wenn Sie ein Installations-Image zur Installation von Panther oder Tiger erstellen, werden optionale Systembestandteile nicht in das Image mit aufgenommen. Sie können das ändern, indem Sie neben dem Punkt IMAGE-QUELLE die Schaltfläche ANPASSEN betätigen. Es erscheint ein Dialogfenster zum An- und Auswählen der im Image enthaltenen Systembestandteile (Abbildung 13.2).

- Die neue Karteikarte MODELLFILTER legt fest, auf welchen Macintosh-Computern das zu erstellende Image benutzt werden darf. Die Grundeinstellung ist ALLE COMPUTER VON APPLE ZULASSEN. Nach Anklicken von NUR UNTEN AUFGEFÜHRTE COMPUTER ZULASSEN können Sie die unterstützen Hardware-Modelle entsprechend auswählen. Interessanterweise wird sogar zu jedem Computertyp ein kleines Bild und eine Kurzbeschreibung angezeigt (Abbildung 13.3).

- Sie können festlegen, welcher Name später für den startenden Computer verwendet wird. Hierbei handelt es sich um den Gerätenamen, der auf jedem Mac OS X-System beim Punkt SHARING in System-Einstellungen notiert ist, nicht um den DNS-Namen. Da ja später mehrere Computer von dem gleichen Image booten und der Gerätename entweder bereits als Vorlage in der Image-Quelle eingestellt war oder unkonfiguriert ist (weil bei einer Image-Erstellung von CD ja keine volle Installation mit Namensvergabe stattgefunden hat), muss vermieden werden, dass alle Computer den gleichen Namen bekommen. Normalerweise versucht das System beim ersten Booten per DHCP seinen Computernamen zu ermitteln. Gelingt dies nicht, werden je nach Betriebssystemversion Namen wie *Default* oder *Macintosh* verwendet, die durch nachgestellte Nummern im Netz eindeutig gemacht werden.

  Das System-Image-Dienstprogramm bietet jedoch auf der Karteikarte SHARING neue Möglichkeiten, den Namen zu vergeben: Entweder Sie geben einen Namen in das Feld COMPUTERNAME an. In diesem Fall wird dieser Name verwendet und die MAC-Adresse des später installierten Computers hinten angehängt. Alternativ können Sie bei DATEIPFAD eine Datei angeben, die der installierte Computer zur Wahl seines eigenen Namens verwenden soll. Es muss sich um eine Textdatei handeln, die zeilenweise die MAC-Adressen und die gewünschten Namen auflistet, wobei beide Angaben jeweils durch ein Tabulatorzeichen zu trennen sind.

- Auf der neuen Karteikarte VERZEICHNISDIENSTE lässt sich einstellen, an welchen Verzeichnisdienst der später fernstartende Computer gebunden werden

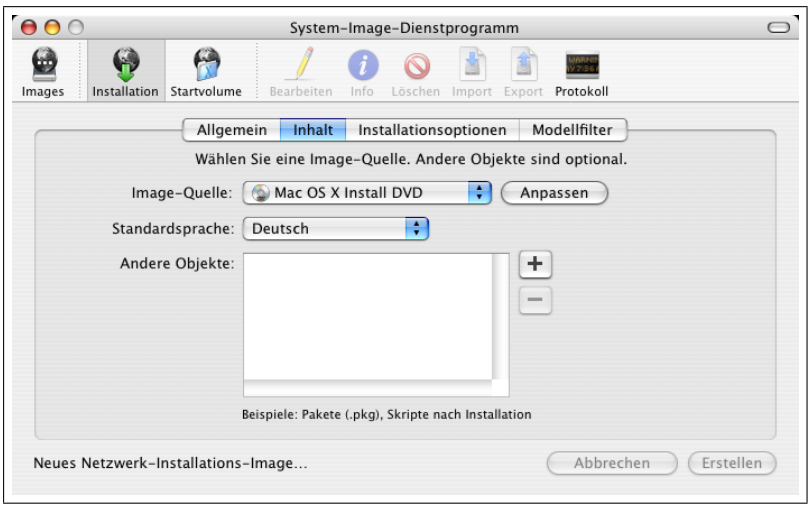

Abbildung 13.2: Die Benutzerführung zur Erstellung eines Installations-Image wurde überarbeitet.

soll. Als Grundlage hierfür wird die Verzeichnisdienstkonfiguration des Computers verwendet, auf dem das System-Image-Dienstprogramm gerade läuft. Kreuzen Sie entweder den Punkt DIE VERZEICHNISDIENSTE-EINSTELLUNGEN DIESES COMPUTERS AUF ALLE CLIENTS ANWENDEN an, um die aktuelle Konfiguration unverändert in das Image hinein zu kopieren, oder betätigen Sie die Schaltfläche IDENTIFIZIEREN... um einen bestimmten (anderen) Verzeichnisknoten auszuwählen. Hierbei lassen sich allerdings auch nur Konfigurationen auswählen, auf die der aktuell vorliegende Computer gerade zugreifen kann.

- Der automatische Namensvorschlag für die nbi-Ordner hat sich geändert. Er hat jetzt den Aufbau *Image_xmmddhhnn*, wobei *x* die vergebene Identifikationsnummer des Images, *mm* der aktuelle Monat, *dd* der Tag und *hhnn* die Erstellungsuhrzeit sind.

13.3 Image-Dateien pflegen und anpassen

Im Hauptbuch hatten wir verschiedene Techniken erläutert, ein bereits vorhandenes NetBoot-Image zu aktualisieren, beispielsweise wenn Apple ein Betriebssystem-Update herausbringt. Auch diese Aufgabenstellung hat Apple in der neuen Version des System-Image-Dienstprogramms stärker als vorher berücksichtigt. Es gibt zwei neue Vorgehensweisen, mit denen Sie ein vorhandenes Image aktualisieren können. Sie müssen allerdings beachten, dass die neuen Funktionen in der hier beschriebenen Form nur dann zur Verfügung stehen, wenn Sie das System-Image-Dienstprogramm *direkt auf dem Server* laufen lassen, der als NetBoot-Server dient.

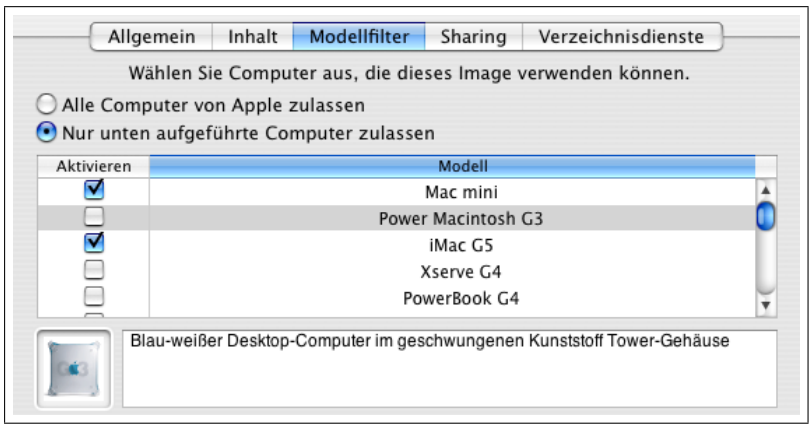

Abbildung 13.3: Die Benutzerführung zum Einstellen des neuen Modellfilters hat Apple fast wie einen Produktkatalog gestaltet.

Im Gegensatz zu den anderen Funktionen können Sie also keinen Administratorrechner verwenden, um die Funktion ferngesteuert übers Netzwerk auszuführen. Hat der Server keine Grafikkarte oder Monitor, wie es bei den aktuellen Xserve-Modellen üblich ist, müssen Sie entweder über die ferne Kommandozeile (SSH) arbeiten oder Fernsteuerungssoftware wie z.B. Apple Remote Desktop verwenden.

13.3.1 Hinzufügen von Paketen zu einem vorhandenen Image

Bei dieser Technik gehen wir davon aus, dass die Software, mit der Sie ein vorhandenes Image aktualisieren möchten, in Form einer Mac OS X-Paketes (pkg) vorliegt. Dies entspricht der üblichen Art und Weise, in der Apple Updates zu Mac OS X ausliefert. Beispielsweise haben Sie von einer Original-Tiger-DVD ein NetBoot-Installations-Image von Version 10.4 erstellt und möchten dieses jetzt auf Mac OS X 10.4.2 aktualisieren. Hierzu laden Sie von Apple das Combo-Update-Paket 10.4.2 von Mac OS X herunter und speichern es als pkg-Datei in einem zugänglichen Ordner auf dem Server.

1. Deaktivieren Sie das zu aktualisierende Image, um zu verhindern, dass Clients es während der nachfolgenden Prozedur benutzen. Melden Sie sich hierzu direkt auf dem NetBoot-Server als Administrator an und stellen Sie sicher, dass kein Client im Moment die NetBoot-Funktion nutzt.

2. Starten Sie Server Admin und wählen Sie in der Tabelle COMPUTER & DIENSTE den Punkt NETBOOT aus.

3. Gehen Sie in der rechten Hälfte des Fensters zu EINSTELLUNGEN und wählen Sie dort den Punkt IMAGES aus.

4. Wählen Sie das Image aus, das aktualisiert werden soll und entfernen Sie das Häkchen AKTIV, um es vorübergehend abzuschalten. Drücken Sie auf SICHERN rechts unten.

5. Starten Sie das System-Image-Dienstprogramm und wählen in der Symbolleiste den Punkt IMAGES aus. Es erscheint eine Liste der auf diesem Server vorhandenen Images.

6. Wählen Sie das zu aktualisierende Image aus und betätigen Sie die Schaltfläche BEARBEITEN in der Symbolleiste.

7. Entscheiden Sie, ob Sie eine Sicherungskopie des Images anlegen wollen. Wir gehen hier davon aus, dass Sie NEIN drücken. Falls Sie JA auswählen, wird vorher eine vollständige Kopie des nbi-Ordners in einem von Ihnen gewählten Zielordner erstellt. Das Programm fragt nach dem Kennwort des Systemverwalters.

8. Warten Sie, bis die Meldung IMAGE BEREIT ZUR BEARBEITUNG links unten im Fenster erscheint. Intern führt das Programm einen Mount auf die ausgewählte Image-Datei aus.

9. Wenn Sie die Betriebssystemversion durch Aktualisieren ändern, möchten Sie wahrscheinlich den Beschreibungstext des Images anpassen. Geben Sie unter ALLGEMEIN in das Feld BESCHREIBUNG auf Wunsch einen überarbeiteten Text ein.

10. Gehen Sie zum Punkt INHALT und drücken Sie die Plus-Schaltfläche neben der Tabelle ANDERE OBJEKTE.

11. Wählen Sie die pkg-Datei mit der Aktualisierung aus, die Sie vorbereitet haben.

12. Klicken Sie auf SICHERN rechts unten. Das Programm führt eine Aktualisierungsinstallation auf dem gemounteten Image durch.

13. Wenn der Vorgang abgeschlossen ist, können Sie in das Programm Server Admin zurückgehen und das Image durch Ankreuzen von AKTIV wieder verfügbar machen.

Die Überarbeitung des Beschreibungstextes ist zwar im Programm vorgesehen, funktioniert aber im Moment nicht richtig. Möglicherweise behebt Apple diesen Fehler in zukünftigen Versionen des System-Image-Dienstprogramms.

13.3.2 Hinzufügen durch Synchronisation

Eine alternative Art und Weise, ein Image zu aktualisieren, bietet sich dann an, wenn Sie ein Image mit einem Startvolume auf Basis einer Festplatte erstellt hatten, die eine „Muster-Installation" enthielt. Sie können in diesem Fall die Platte, die als Vorlage dient, nach Ihren eigenen Wünschen aktualisieren, ohne unbedingt auf pkg-Dateien angewiesen zu sein. Das System-Image-Dienstprogramm kann dann auf Basis des geänderten Platteninhalts ein vorhandenes Image durch *Synchronisation* auf den neuesten Stand bringen.

1. Stellen Sie genau wie im letzten Abschnitt beschrieben sicher, dass niemand im Moment mit dem zu aktualisierenden Image arbeitet, indem Sie es in Server Admin deaktivieren.
2. Schließen Sie die Platte an den Server an, auf der sich das bereits nach Ihren Wünschen angepasste Mustersystem befindet. Vorsicht: Es muss sich wirklich um genau die Vorlage handeln, die ursprünglich einmal verwendet wurde, um das Image zu erstellen, das jetzt aktualisiert werden soll. Falls es sich um das falsche Volume handelt, kann die Synchronisation fehlschlagen und das Image wird unbrauchbar.
3. Starten Sie das System-Image-Dienstprogramm und wählen Sie den Menüpunkt SYSTEM-IMAGE-DIENSTPROGRAMM | EINSTELLUNGEN.
4. Schalten Sie in der unteren Hälfte des Einstellungsfensters die Option OBJEKTE HINZUFÜGEN UND QUELLE SYNCHRONISIEREN ein. Schließen Sie das Einstellungsfenster wieder.
5. Klicken Sie den Punkt IMAGES in der Symbolleiste an.
6. Wählen Sie das zu aktualisierende Image aus und klicken dann auf den Punkt BEARBEITEN in der Symbolleiste. Das Programm fragt nach dem Kennwort des Systemverwalters.
7. Gehen Sie zur Rubrik INHALT.
8. Wählen Sie im Klappmenü IMAGE-QUELLE die Festplatte aus, die das aktualisierte Mustersystem enthält.
9. Drücken Sie auf SICHERN rechts unten.
10. Wenn der Vorgang abgeschlossen ist, können Sie das Image im Server Admin-Programm wieder verfügbar machen.

Kapitel 14

Fortgeschrittene Netzfunktionen

14.1 Der neue Software-Aktualisierungsdienst

14.1.1 Einführung

Eine komplett neue Entwicklung von Apple ist der *Software-Aktualisierungsdienst*, der in Tiger Server zum ersten Mal zum Einsatz kommt. Diese Funktion erlaubt es, die Mac OS X Software-Aktualisierung, die auf jedem System als Teil des Programms Systemeinstellungen abrufbar ist, auf einen eigenen Server im Hause umzuleiten, wobei Apples offizieller Update-Server gespiegelt wird. Dies bringt folgende Vorteile:

- Sie können verhindern, dass Benutzer in Ihrem Netz, die lokale Administrationsrechte haben, ohne Genehmigung Software-Updates von Apple einspielen und damit Probleme verursachen.
- Sie sparen Internet-Bandbreite, denn nur noch ein einziger Rechner ruft die aktuellen Software-Updates von Apple ab. Danach können die Pakete per LAN im Haus verteilt werden.
- Es besteht stets eine aktuelle Kontrolle, welche Software-Updates Apple momentan anbietet und ob Sie diese in Ihrem Netz einsetzen möchten.
- Für die Endbenutzer im Netz ist dies ein völlig transparenter Vorgang, denn sie können nicht unterscheiden, ob die Aktualisierungen von Apple oder aus dem Hausnetz herunter geladen werden.

Nachdem Sie den Software-Aktualisierungsdienst auf einem Mac OS X Server eingeschaltet haben, beginnt der betreffende Computer in regelmäßigen Abständen

durch Internet-Anfragen bei Apple festzustellen, welche Update-Pakete zur Verfügung stehen. Wenn neue Pakete entdeckt werden, werden diese automatisch herunter geladen und auf dem Server zwischengespeichert. (Die Server-Software selbst wird hierbei nicht aktualisiert.) Durch Verwendung der Verzeichnisdienstfunktion *Verwaltete Einstellungen* können Sie bestimmte oder alle Computer in Ihrem lokalen Netz dazu zwingen, die Software-Aktualisierungsfunktion von Mac OS X nicht mehr durch Anfragen bei Apple zu realisieren, sondern die Anfragen auf Ihren eigenen Server umzuleiten. Hierbei können Sie zentral auf dem Server bestimmen, welche Pakete den Klienten angeboten werden sollen. Insbesondere lässt sich auch sperren, dass die Clients bestimmte Pakete zu Gesicht bekommen. Da Apples Aktualisierungen oftmals Defekte enthalten und zu Kompatibilitätsproblemen führen können, haben Sie damit die Chance, die automatische Aktualisierung bestimmter Programme zu verhindern. Sie können die automatische Installation zentral gesteuert so lange verzögern, bis Sie das Paket selbst getestet und als unbedenklich eingestuft haben.

Neben Updates im Zusammenhang mit Mac OS X sind auch alle anderen Software-Produkte von Apple Teil des Aktualisierungsdienstes. Updates von Drittanbietern werden über diesen Mechanismus nicht unterstützt. Die Authentizität der Software wird dadurch gesichert, dass alle Pakete mit digitalen Signaturen versehen sind, die über Apples Server einzeln geprüft werden. Auch der Fall, dass Apple ein Paket aus Sicherheitsgründen zurückziehen muss, ist vorgesehen: Bei der Synchronisierung kann Apple bewirken, dass ein mangelhaftes Update-Paket auf den Spiegelservern wieder gelöscht wird.

Der Software-Aktualisierungsdienst ist ein neues Produkt und als solches in einigen Punkten noch etwas unausgegoren. Es gibt im Moment folgende Schwächen:

- Es gibt keine Möglichkeit, den Ablageort für die Update-Pakete auf dem Server zu beeinflussen. Die Pakete werden fix in den Ordner

  ```
  /usr/share/swupd/html
  ```

  gelegt. Die Speichermenge kann völlig unkontrolliert anwachsen, wobei Platz auf der Systempartition verbraucht wird.

- Es ist zwar möglich, die Download-Bandbreite zwischen Clients und Server, nicht jedoch die Bandbreite zwischen eigenem Server und Apples Server zu begrenzen. Besonders in kleinen Netzen wäre die letztere Einstellung wichtiger, da mehr als 1 GByte Software aus dem Internet geladen werden müssen. Diese Menge wird in Zukunft weiter steigen.

- Es ist zwar möglich, zur Lastverteilung im lokalen Netz mehrere Aktualisierungsserver bereit zu halten, aber diese arbeiten dann völlig autark und koordinieren sich nicht untereinander. Es ist nicht möglich, eine Haupt- und Neben-Server-Hierarchie aufzubauen.

- Die herunter geladenen Pakete können nur im Zusammenhang mit der Software-Aktualisierungsfunktion in Systemeinstellungen verwendet werden. Es ist ohne weiteres nicht möglich, die Pakete z.B. auf DVD zu brennen, um sie auf nicht vernetzte Computer zu übertragen.

- Es gibt keine grafische Schnittstelle, um vorhandene Pakete auf dem Aktualisierungsserver gezielt zu löschen. Sie können nur deaktiviert werden. Auch das Löschen über die Kommandozeile ist schwierig, da alle Dateien unter verschlüsselten Namen abgespeichert werden.
- Die Funktion steht ausschließlich für Klienten ab Mac OS X Version 10.4 zur Verfügung. Ältere Systeme und Software-Produkte werden nicht aktualisiert.

Im Zuge der Kapazitätsplanung Ihres Netzes sollten Sie berücksichtigen, dass die Anforderungen beim Einsatz des Software-Aktualisierungsdienstes ähnlich sind, wie beim Betrieb eines NetBoot-Servers. Nähere Hinweise finden Sie in Abschnitt 13.1 des Hauptbuchs.

14.1.2 Einrichten der Software-Aktualisierungsfunktion

Die Einrichtung des Dienstes besteht aus zwei Teilen: Zum einen müssen Sie den Spiegelungsserver einrichten, der die Update-Pakete speichert, zum anderen müssen Sie über verwaltete Einstellungen die Client-Computer anweisen, diesen Spiegelungsserver als Aktualisierungsserver zu verwenden.

1. Starten Sie das Programm Server Admin und verbinden Sie sich mit dem Server, der die Aktualisierungspakete beherbergen soll.
2. Wählen Sie in der Tabelle COMPUTER & DIENSTE den Punkt SOFTWARE-AKTUALISIERUNG aus.
3. Gehen Sie auf der rechten Seite des Fensters zum Punkt EINSTELLUNGEN, Karteikarte ALLGEMEIN.
4. Kreuzen Sie den Punkt UPDATES VON APPLE AUTOMATISCH SPIEGELN an.
5. Falls Sie alle Aktualisierungspakete, die Apple anbietet, ungeprüft auf die Clients übernehmen möchten, kreuzen Sie den Punkt GESPIEGELTE UPDATES AUTOMATISCH AKTIVIEREN an. Die sicherere Einstellung ist jedoch, diesen Punkt auszuschalten. In diesem Fall müssen Sie selbst in regelmäßigen Abständen die Liste der vorhandenen Pakete durchgehen und einzeln prüfen, welche Sie in Ihrem Hausnetz anbieten möchten. Erst wenn Sie ein Paket von Hand aktivieren, können Ihre Klienten darauf zugreifen.
6. Falls Sie die Bandbreite zwischen einem Client und diesem Server beim Herunterladen der Software-Aktualisierung begrenzen möchten, kreuzen Sie den Punkt BANDBREITE FÜR UPDATES BEGRENZEN AUF an und geben Sie den gewünschten Wert an. Der Wert ist *pro Client* gemeint. Wenn Sie also 10 Client-Computer haben und die Bandbreite auf 50 KB/s begrenzen, werden im Extremfall insgesamt 500 KB/s auf dem Server beansprucht, wenn alle Clients gleichzeitig Software herunterladen. Beachten Sie, dass es durch regelmäßigen Betriebsablauf und die Funktionsweise der Software-Aktualisierung in Systemeinstellungen sehr wahrscheinlich ist, dass alle Clients die Software zur gleichen Zeit abrufen.

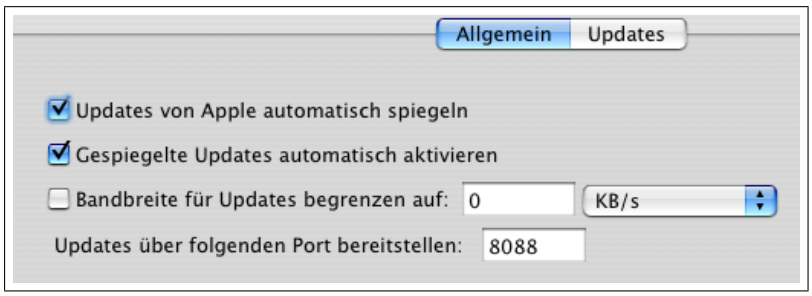

Abbildung 14.1: Wenn Sie den zweiten Punkt ankreuzen, stehen alle von Apple angebotenen Pakete sofort auf den Clients zur Verfügung. Schalten Sie diese Option ab, haben Sie die Gelegenheit, die Pakete manuell zu prüfen. Sie können so verhindern, dass sich Kompatibilitätsprobleme oder Probleme mit fehlerbehafteten Updates ergeben.

7. Wenn Sie einen speziellen Port definieren möchten, auf dem das Herunterladen in Ihrem Netz erfolgen soll, können Sie die Portnummer bei UPDATES ÜBER FOLGENDEN PORT BEREITSTELLEN eingeben. Im Normalfall bleibt der Wert *8088* eingestellt. Falls Sie den Wert ändern, müssen Sie dies natürlich weiter unten bei der Konfiguration der Clients berücksichtigen. Zum Sharing der Aktualisierungspakete verwendet Mac OS X einen Mini-HTTP-Server, der von den restlichen Web-Diensten unabhängig ist.
8. Sind alle Werte eingestellt, betätigen Sie die Schaltfläche SICHERN rechts unten im Fenster.
9. Klicken Sie auf DIENST STARTEN in der Symbolleiste, um die Software-Aktualisierung in Gang zu setzen. Das System wird nach kurzer Zeit beginnen, Apples Software-Aktualisierungspakete auf diesen Server zu spiegeln. Je nach Geschwindigkeit Ihrer Internet-Leitung wird dies mehrere Minuten oder Stunden benötigen.

Sie können die Tätigkeit des Dienstes beobachten, indem Sie den Punkt PROTOKOLL auswählen. Die Liste der einzelnen Pakete können Sie einsehen, wenn Sie bei EINSTELLUNGEN auf die Karteikarte UPDATES wechseln (Abbildung 14.2). Wichtig ist hier die Einstellung in der Spalte AKTIV, die für jedes Paket entscheidet, ob die Klienten in Ihrem Netz das Paket „sehen“ und herunter laden dürfen. Sie können eine sofortige Synchronisation der Pakete zwischen diesem Server und Apples Server erzwingen, indem Sie die Schaltfläche JETZT SUCHEN betätigen. Die Uhrzeit des letzten Suchvorgangs wird unter der Tabelle hinter LETZTE PRÜFUNG angezeigt.

Wenn Sie sehen, dass Ihr Server alle Pakete komplett gespiegelt hat und damit auf dem aktuellen Stand ist, können Sie die Clients anweisen, Ihren Hausserver als offiziellen Update-Server zu verwenden. Hierzu richten Sie eine entsprechende verwaltete Einstellung ein, die Sie an die betreffenden Netzwerkkonten binden. Es bietet sich an, hierfür ein Computerlistenkonto zu verwenden, das alle Clients einschließt.

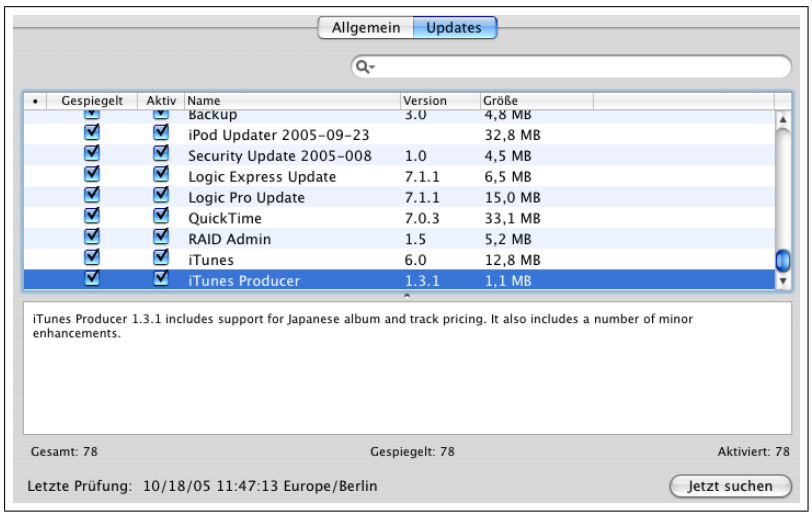

Abbildung 14.2: Die Liste der Update-Pakete wird angezeigt. Im Laufe der Zeit kommt über 1 GByte an Software zusammen. Über die Spalte AKTIV können Sie steuern, ob Sie das jeweilige Paket zum Einsatz auf Ihren Klienten freigeben möchten.

1. Starten Sie das Programm Arbeitsgruppen-Manager und verbinden Sie sich mit dem Server, auf dem der Open Directory-Dienst läuft, an den Ihre Klienten gebunden sind.

2. Sorgen Sie dafür, dass der richtige Verzeichnisknoten für netzweite Verwaltung ausgewählt ist und melden Sie sich über das Schlosssymbol bei diesem Knoten an.

3. Klicken Sie in der Symbolleiste auf den Punkt EINSTELLUNGEN.

4. Wählen Sie in der linken Hälfte das Konto aus, an das die Einstellung der Software-Aktualisierung gebunden werden soll (siehe auch Abschnitte 5.7.5 und 5.7.6 des Hauptbuchs).

5. Wählen Sie rechts den Punkt SOFTWARE-AKTUALISIERUNG aus.

6. Stellen Sie die Option VERWALTEN auf IMMER.

7. Geben Sie bei ZU VERWENDENDER SOFTWARE-UPDATE-SERVER die Adresse des Servers an, den Sie oben als Spiegelserver konfiguriert hatten. Es handelt sich um eine URL der Form

   ```
   http://servername:8088/
   ```

   Hierbei ist `servername` durch den DNS-Namen oder die IP-Adresse des Aktualisierungsservers zu ersetzen und 8088 durch die Portnummer, die Sie bei der Einrichtung des Servers ausgewählt haben (Abbildung 14.3).

Abbildung 14.3: Die Client-Computer verwenden Ihren lokalen Aktualisierungsdienst nur dann, wenn sie über eine verwaltete Einstellung dazu gezwungen werden. Es reicht die Angabe der URL.

8. Betätigen Sie die Schaltfläche FERTIG.

Wenn auf einem der betroffenen Client-Computer nun automatisch oder manuell der Punkt SOFTWARE-AKTUALISIERUNG in Systemeinstellungen aufgerufen wird, verbindet er sich nicht mehr mit Apple, sondern mit Ihrem eigenen Server. Die Pakete, die in der Liste als aktiv markiert sind, werden angeboten und können installiert werden.

14.2 Verschlüsselte Teilnetze mit VPN

Wie in Kapitel 14.2.1 des Hauptbuchs beschrieben, war Mac OS X Server bisher darauf beschränkt, bei der Nutzung von VPN-Funktionen einzelnen, sich in das Hausnetz einwählenden Computern eine verschlüsselte Verbindung zur Verfügung zu stellen. In Tiger wurde diese Funktion erweitert: Es ist jetzt auch möglich, zwei komplette Teilnetze über ein VPN miteinander zu verbinden. Diese Betriebsart wird *Site-to-Site Virtual Private Networking* genannt. Eine solche Konfiguration wird üblicherweise dann gewählt, wenn das Netz einer Firmenfiliale an einem entfernten Standort mit dem Netz der Firmenzentrale verbunden werden muss. Dank der Verschlüsselung kann das unsichere Internet zur Verbindung der beiden Netze zum Einsatz kommen, ohne dass teure Standleitungen zwischen beiden Orten geschaltet werden müssen.

Abbildung 14.4 zeigt, wie eine solche Konfiguration in der Praxis aussieht: Es werden zwei Mac OS X Tiger Server benötigt, auf denen jeweils die VPN-Funktionalität eingeschaltet ist. Das Hauptnetz mit eigenem DNS-Server befindet sich an Standort 1, die „Filiale“ mit ihrem Nebennetz befindet sich an Standort 2. Die beiden Netze sind über zwei Router gekoppelt, der Weg dazwischen kann ungesichert sein und wird durch die Verschlüsselung des VPNs geschützt. Das Bild zeigt beispielhaft IP-Adressen, die im Folgenden verwendet werden, um die Einrichtung zu veranschaulichen.

Wir nehmen an, das VPN-Gateway des Standorts 1 – mit anderen Worten der Mac OS X Server, auf dem die VPN-Dienste laufen – ist im öffentlichen Internet über die Adresse 1.2.3.4 erreichbar und der VPN-Server des Standorts 2 kann über

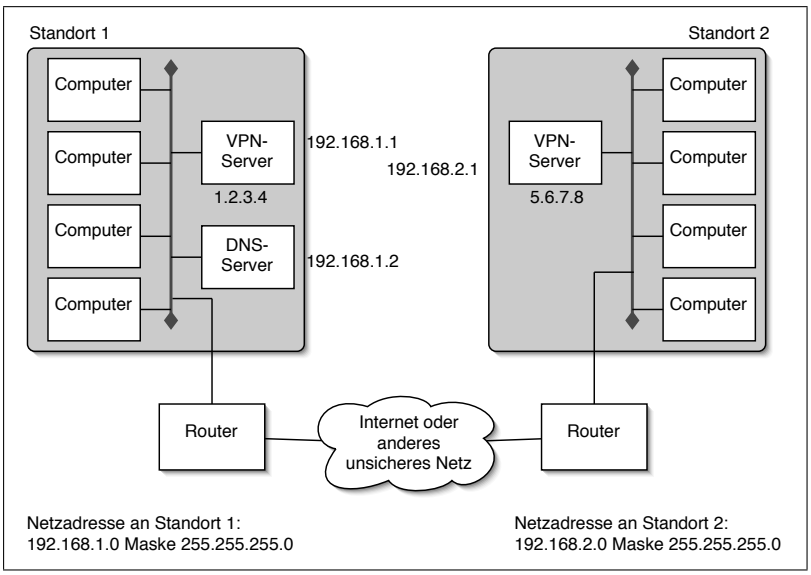

Abbildung 14.4: Die Abbildung zeigt die typische Konfiguration eines Site-to-Site-VPN. Das in diesem Abschnitt erläuterte Fallbeispiel verwendet die im Bild genannten Adressen.

die Adresse 5.6.7.8 erreicht werden. Die Computer am Standort 1 verwenden als Netzadresse die 192.168.1.0 mit der Teilnetzmaske 255.255.255.0, die Computer am Standort 2 verwenden Adressen der Form 192.168.2.0, ebenso mit der Maske 255.255.255.0. Zwischen den beiden Servern wird ein VPN etabliert, das die Daten durch das unsichere Internet tunnelt. Anders als bei der im Hauptbuch beschriebenen VPN-Einwahl benötigen wir an dieser Stelle keinen für das VPN reservierten privaten Adressbereich. Wie technisch die Daten verschlüsselt zwischen den Internet-Adressen 1.2.3.4 und 5.6.7.8 laufen, spielt für die Konfiguration keine Rolle. Intern wird hierzu *L2TP über IPSec* verwendet.

Im folgenden Beispiel gehen wir davon aus, dass ein *Shared Secret* zur Verschlüsselung verwendet wird. Alternativ könnte auch ein Zertifikat zum Einsatz kommen, was sich insbesondere anbietet, wenn ein VPN-Server gleich mit *mehreren* Site-to-Site-Netzen in Verbindung steht. Außerdem setzen wir voraus, dass auf beiden Servern bereits ein Firewall-Dienst eingeschaltet ist und die Filterregeln an das jeweilige Hausnetz und die in Betrieb befindlichen Dienste an beiden Standorten angepasst sind.

In der unten stehenden Anleitung werden einige Konfigurationsschritte an der Firewall mithilfe der deutschen Oberfläche von Server Admin erklärt. Bis Redaktionsschluss wies jedoch die deutschsprachige Oberfläche von Tiger einen Fehler auf, der die Einrichtung einer Filterregel für Sonderprotokolle verhindert. Dies betrifft die Schritte am Schluss, bei denen Filterregeln für die Protokolle *esp* und *ipencap* definiert werden: Das Textfeld zur Eingabe des Protokollnamens ist in der deutschen Version inaktiv geschaltet, so dass Sie gar nichts eingeben können.
Solange Apple diesen Fehler nicht behoben hat, müssen Sie Server Admin für die Ausführung dieser Schritte auf den Betrieb in englischer Sprache schalten. Beenden Sie hierzu Server Admin, starten Sie das Programm Systemeinstellungen, öffnen Sie den Punkt LANDESEINSTELLUNGEN und schieben Sie in der Tabelle SPRACHE mit der Maus den Eintrag ENGLISH an die oberste Position. Starten Sie danach Server Admin wieder. Nach Abschluss der Konfigurationsarbeiten können Sie die Sprachentabelle zurück auf Normalbetrieb setzen, indem Sie DEUTSCH wieder an die oberste Stelle schieben.

Die erste Phase der Konfiguration kann nur über die Kommandozeile vorgenommen werden. Hierzu wird das Programm *s2svpnadmin (Site-to-Site Virtual Private Network Administration)* verwendet.

1. Öffnen Sie ein Terminal-Fenster auf dem Server und geben Sie den Befehl

   ```
   sudo s2svpnadmin
   ```

   ein. Geben Sie Ihr Kennwort ein, wenn das System danach fragt.

2. Wählen Sie im Auswahlmenü den Punkt (3), um eine neue Site-to-Site-Verbindung einzurichten.

3. Geben Sie einen neuen Konfigurationsnamen ein, wobei Sie kein Leerzeichen oder Sonderzeichen verwenden dürfen, z.B. *standort1*.

4. Geben Sie die öffentliche IP-Adresse des lokalen Servers ein, in diesem Fall 1.2.3.4.

5. Geben Sie die öffentliche IP-Adresse des entfernt stehenden Servers ein, in diesem Fall 5.6.7.8.

6. Wählen Sie s um die Verwendung eines Shared Secrets zu bestätigen.

7. Geben Sie das Shared Secret ein.

8. Nun werden die Adressierungsrichtlinien für das VPN eingestellt. Geben Sie zuerst die Netzwerkadresse des diesseitigen Netzes ein, hier 192.168.1.0.

9. Geben Sie die zugehörige Netzmaske an, indem Sie die Anzahl der Bits eintragen. (Siehe hierzu auch Abschnitt 3.2.9 im Hauptbuch). In diesem Fall sind es 24 Bits.

10. Geben Sie jetzt die Netzwerkadresse des fernen Netzes an, in diesem Fall 192.168.2.0.

11. Geben Sie die entsprechende Netzmaske, hier wieder 24 Bits an.

12. Beantworten Sie die Frage DO YOU WANT TO ADD NEW POLICIES? mit n. In diesem Fall sind keine weiteren Adressierungsregeln nötig. Weitere Regeln könnten erforderlich sein, wenn Sie beispielsweise nur Teilnetze der beiden Standorte miteinander verknüpfen wollten.

13. Bestätigen Sie durch Eingabe von y, dass diese Konfiguration aktiviert werden soll. Das Programm sollte mit SUCCESSFULLY ADDED SERVER antworten.

14. Beenden Sie das Programm durch Auswahl des Menüpunktes (5).

15. Wiederholen Sie alle Schritte nun auf dem zweiten Server am zweiten Standort. Hierbei sind die Rollen von lokalem und fernen Netz natürlich alle zu vertauschen.

16. Öffnen Sie das Programm Server Admin an Standort 1 und verbinden Sie sich mit dem lokalen Server. Wählen Sie in COMPUTER & DIENSTE den Punkt FIREWALL aus.

17. Gehen Sie zum Punkt EINSTELLUNGEN, dort zu ADRESSGRUPPEN.

18. Fügen Sie mit der Plus-Schaltfläche unterhalb der Tabelle eine Adressgruppe hinzu. Als Name können Sie beispielsweise *Standort1* verwenden. Ersetzen Sie die Adresse *any* durch die CIDR-Angabe *1.2.3.4/32*.

19. Fügen Sie mit der Plus-Schaltfläche unterhalb der Tabelle eine weitere Adressgruppe hinzu. Als Name können Sie beispielsweise *Standort2* verwenden. Ersetzen Sie die Adresse *any* durch die CIDR-Angabe *5.6.7.8/32*.

20. Wählen Sie die Adressgruppe BELIEBIG (ANY). Kreuzen Sie auf der Karteikarte DIENSTE an, dass Sie den Verkehr VPN L2TP - LAYER TWO TUNNELING PROTOKOLL auf Port 1701 zulassen und drücken Sie SICHERN.

21. Wechseln Sie auf die Karteikarte ERWEITERT und drücken Sie die Plus-Schaltfläche unterhalb der Tabelle.

22. Fügen Sie eine erweiterte Regel mit folgenden Einstellungen hinzu: AKTION: ERLAUBEN, PROTOKOLL: *UDP*, QUELLE: ADRESSE: *Standort1*, ZIEL: ADRESSE: *Standort2*, SCHNITTSTELLE: ANDERE: *isakmp*. Diese Regel erlaubt den Schlüsselaustausch für IPSec von diesem zum entfernten Server.

23. Fügen Sie eine erweiterte Regel mit folgenden Einstellungen hinzu: AKTION: ERLAUBEN, PROTOKOLL: *UDP*, QUELLE: ADRESSE: *Standort2*, ZIEL: ADRESSE: *Standort1*, SCHNITTSTELLE: ANDERE: *isakmp*. Diese Regel erlaubt den Schlüsselaustausch für IPSec vom entfernten zu diesem Server.

24. Fügen Sie eine erweiterte Regel mit folgenden Einstellungen hinzu: AKTION: ERLAUBEN, PROTOKOLL: ANDERES: *esp*, QUELLE: ADRESSE: *Standort1*, ZIEL: ADRESSE: *Standort2*. Diese Regel erlaubt die Verwendung des Protokolls *Encapsulating Security Payload*.

25. Wiederholen Sie den letzten Schritt, wobei Sie die Quell- und Zieladressen vertauschen.

26. Fügen Sie eine erweiterte Regel mit folgenden Einstellungen hinzu: AKTION: ERLAUBEN, PROTOKOLL: ANDERES: *ipencap*, QUELLE: ADRESSE: *Standort1*, ZIEL: ADRESSE: *Standort2*. Diese Regel erlaubt die Übertragung von (verschlüsselten) IP-Paketen, die andere IP-Pakete enthalten.

27. Wiederholen Sie den letzten Schritt, wobei Sie die Quell- und Zieladressen vertauschen.

28. Stellen Sie sicher, dass bei den sechs neu hinzugefügten Regeln jeweils das Häkchen AKTIV gesetzt ist.

29. Klicken Sie auf die Schaltfläche SICHERN rechts unten und starten Sie die Firewall neu.

30. Wiederholen Sie alle Konfigurationsschritte für die Firewall auf dem Server an Standort 2.

31. Kontrollieren Sie, ob der VPN-Dienst an beiden Standorten läuft. Falls nicht, schalten Sie ihn auf beiden Seiten durch Klick auf DIENST STARTEN in der Symbolleiste von Server Admin ein. Es ist nicht nötig, dass Sie an den VPN-Einstellungen in Server Admin etwas ändern oder hinzufügen. Sie werden auch keine Verbindungsmeldungen oder Protokolleintragungen für den Site-to-Site-Betrieb an dieser Stelle abrufen können. Nur das Einschalten des VPN-Dienstes ist wichtig.

Danach ist die Verbindung zwischen beiden Netzen eingerichtet. Sie können beispielsweise über die Kommandozeile oder über das Netzwerk-Dienstprogramm von einem Rechner an Standort 1 ein *Ping* an einen Rechner an Standort 2 senden, um die Konnektivität zu testen.

Index

Öffentliche Ansicht, 90
3GPP, 178
3rd Generation Partnership Project, 178
64-Bit-Technologie, 3

Access Control Entry, 32
Access Control Lists, 7, 31
ACE, 32
ACL, 7, 31
AFP-zu-NFS-Resharing, 99
AIM, 172
AMD, 103
Apache, 157
AppleShare, 18
AppleShare IP, 66
AppleTalk, 18
asr, 50
Automator, 6

Backup Domain Controller, 100
Bayes, Thomas, 148
BDC, 100
benannte Ansicht, 90
Blog, 166
Bloggen, 163
Blojsom, 7, 163
Bonjour, 107

CA, 120
Certificate Authority, 120
Certificate Revocation List, 124
Chat-Namen, 172
Chat-Server, 172
Chatten, 171
chmod, 47
ClamAV, 7, 148
Computer, 90
Computerkonto, 88
CRL, 124
cron, 4
Cyrus, 143

DansGuardian, 159
Darwin Streaming Server, 178
Dashboard, 6
DG Console, 159
diradmin, 19
ditto, 50
Drucker-Dienstprogramm, 141
Druckerpool, 140
Dynamische Liste, 90

Einstellungsdomäne, 77
Einstellungsmanifest, 84
Eintrag (Weblog), 167
Encapsulating Security Payload, 202
Extensible Messaging and Presence Protocol, 173

FFAgent, 107
FIPS 181, 63
Forwarder, 24
fsaclctl, 50

geerbte Gruppe, 45
Generated Unique Identifier, 33
Globally Unique Identifier, 33
Globally Unique Naming, 77
Grapher, 6
gTLD, 23
GUID, 33

H.264, 178
HD, 178
High Definition, 178

iChat, 171, 175
iChat-Server, 7, 172

init, 4
Instant Messaging, 171
IPP, 139
ISO 14496-10, 178
ITU-T H.264, 178

Jabber, 172
Jabber / XMMP, 173
jabberd, 7, 173

Kategorie (Weblog), 167
Kennwortassistent, 63
Kindersicherung, 72

L2TP über IPSec, 199
Latente Semantische Analyse, 148
Launch Daemon, 4
launchd, 4
Link Aggregation, 8
loginwindow, 80
Lopata, Dave, 159
ls, 47
LSA, 148

mach_init, 4
Macintosh Manager, 19
main.cf, 143
MD5, 14
mdimport, 162
mdutil, 162
Mobiler Benutzer, 53
mod_sherlock_apple, 162
mod_spotlight_apple, 162
MPEG-4 Teil 10, 178

netatalk, 19
NetWare, 19
Netzwerk-Image-Dienstprogramm, 185
Netzwerkansicht, 90
Netzwerkordner, 86
Netzwerkumgebung, 90
Nickname, 174
NTLMv2, 59

OCSP, 124
Online Certificate Status Protocol, 124
Open Directory Replik, 102

p12, 134
PAC-Datei, 15
PDC, 102
Ping, 202
plist-Dateien, 4
Primärer Domänen-Controller, 102
Property List Editor, 77
Property Lists, 4
Protokolle, 140
Pseudonym, 174

QTSS, 177
QTSS Publisher, 178
Quartz Extreme 2D, 1
QuickTime Streaming Server, 177

rückführbare Identifizierungsmethoden, 60
Rückverbindung, 168
Really Simple Syndication, 6
Rendezvous, 107
Retrospect, 51
root, 20
Root Certificate Authority, 120
RSS, 6

s2svpnadmin, 200
SACL, 37
Schlüsselbund, 119
Service Access Control List, 37
Service Recovery, 18
Shared Secret, 199
Sherlock, 162
Sicherungs-Domänen-Controller, 100
Site-to-Site Virtual Private Networking, 198
Site-to-Site-VPN, 8
Software-Aktualisierungsdienst, 193
SourceForge, 160
SPAM, 143
SpamAssassin, 7, 148
Spotlight, 5, 34
Squid, 159
squid, 15
Standardansicht, 90
Synchronisation, 192
System Profiler, 1
System-Image-Dienstprogramm, 185
Systembibliothek, 179

Telefax, 14
template.spotlight, 163
TextEdit, 78
Trackback, 168
Trainingsphase, 148
Trusted Binding, 115

UCE, 143

Vertrauenswürdige Bindung, 115
Verwaltete Einstellungen, 194
Verwaltete Netzwerkansicht, 87
Verzeichnisbindung, 115
Verzeichnisdienste, 109
Verzeichnisreplikation, 100
virtueller Host, 143
VoiceOver, 6
VPN, 198

Weblog, 166
WebObjects, 7, 157
Windows NT Server, 19

X509Anchors, 120
Xgrid, 7
xinetd, 4
XMMP, 173

ZeroConf, 107
Zertifikatsassistent, 129
Zertifikatsaussteller, 120
Zugriffsrecht, übernommenes, 36
Zugriffsrecht, explizites, 36
Zugriffssteuerungseintrag, 32
Zugriffssteuerungslisten, 7, 31
Zurückgezogenes Zertifikat, 124